AFRL-SR-AR-TR-02-0169

Novel Mathematical/Computation Approaches to Image Exploitation

F49620-00-C-0020

Dr. Richard Tolimieri, PhD
Massachusetts Technological Laboratory, Inc.

May 3, 2002

20020614 191

Approved for public release; distribution unlimited

Air Force Research Laboratory
Air Force Office of Scientific Research
Arlington, Virginia

REPORT DOCUMENTATION PAGE

AFRL-SR-AR-TR-02-

0169

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching exi the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions fc Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Rec

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYP.
		15 APR 00 - 14 APR 02

4. TITLE AND SUBTITLE
NOVEL MATHEMATICAL/COMPUTATION APPROACHES TO IMAGE EXPLOITATION

5. FUNDING NUMBERS
F49620-00-C-0020

6. AUTHOR(S)
DR. RICHARD TOLIMIERI

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
MASSACHUSETTS TECHNOLOGICAL LABORATORY, INC.
330 PLEASANT STREET
BELMONT, MA 02478

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFOSR/NM
801 N. Randolph Street Room 732
Arlington, VA 22203-1977

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
F49620-00-C-0020

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE, DISTRIBUTION UNLIMITED

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

During the last ten years considerable effort has taken place to extend the range of applicability of nonabelian group methods to the design of new filters and spectral analysis methodologies (8,9,5), as an image processing tool (11,13,19,20). Many efforts at finding a significant role for nonabelian group theory in DSP and image processing applications as well as in coding and communication theory have been limited by some or all of the following: 1) The choice of an appropriate group or groups in a given application is not obvious. 2) The lack of a large class of groups whose harmonic analysis is sufficiently understood for meaningful applications. 3) The absence of a conceptual framework which relates group harmonic analysis to physically interpretable results. 4) Fast alforithms may exist but are difficult to code as they do not easily lend themselves to modication 5) The lack of relevant models for applications which are not only a rephrasing of known methods or what is immediately available.

14. SUBJECT TERMS	15. NUMBER OF PAGES
	119
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT

Novel Mathematical/Computation Approaches to Image Exploitation

Research and Development Status Report

Final Report: 15 April, 2000 - 14 April, 2002

Contract No. F49620-00-C-0020

Sponsored By

Air Force Office of Scientific Research (DOD)
Defense Small Business Technology Transfer Program

Principal Investigator: Dr. Richard Tolimieri
Contractor: Massachusetts Technological Laboratory, Inc.
Business Address: 330 Pleasant Street, Belmont, MA 02478

Effective Date of Contract: 15 April, 2000
Contract Expiration Date: 14 April, 2002

Submitted By

Dr. Ta-Ming Fang
Massachusetts Technological Laboratory, Inc.
(617)484-2296; (617)484-7314 (Fax)

(05/03/2002)

Disclaimer

The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed, or implied, of the Air force Office of Scientific Research or the U. S. Government.

Contents

1 Summary

Image processing typically involves the processing of large quantities of data by computationally intensive and mathematically complex numerical procedures. A key task in image processing is to search for transforms that faithfully and efficiently represent image data. The choice of a transform in a specific application can depend on a wide range of possibly conflicting criteria, including the nature of the redundancies and noise introduced by sensors and image propagation medium characteristics, the overall accuracy, stability and computational cost of utilizing the transform and the underlying processing strategy.

This report addresses the need to design and implemented application specific algorithms for automated target detection and classification by providing novel image transforms from nonabelian group harmonic analysis. Our methods include procedures for incorporating prior knowledge of target size and shape as inputs to thresh-holding and filtering of spectral coefficients defined by unitary operators associated to nonabelian groups. By operating on spectral coefficients, these operators can be targeted to specific tasks at a level of detail not available in traditional transform methods including Fourier methods, discrete cosine transform methods and more recently developed wavelet methods. When combined with a corresponding analysis of target signal's unique structures and textural properties, our methods provide powerful tools for detection and classification and protection from false detection.

We have investigated the use of group theory for producing transformations that will incorporate several classes of prior image information. Identification of image properties which can be addressed in a group theoretic framework is a part of our ongoing research.

Our efforts have been focused on constructing transforms for discriminating particular geometric properties in images as well as locating the occurrences of such geometry. Encoding of prescribed pattern into an invariant subspace is a design process, based on selection of a nonabelian group. Once this encoding is completed however, locating the pattern is automatic. Compared to methods based on matched filter processing, the nonabelian group projection methods will be global, and can encode multi-dimensional geometric information that are independent of precise pixel values, or pixel-to-pixel variances.

For applications to image processing, especially for composite, iterative processing, the software library of the unitary transforms of complete systems of orthogonal idempotents and associated projection operators are being extended and structured based on both the image processing characteristics and group theoretic properties of the projection operators. These operators are tested extensively for performance in severe additive and multiplicative noises.

2 Introduction

During the last ten years considerable effort has taken place to extend the range of applicability of nonabelian group methods to the design of new filters and spectral analysis methodologies [8, 9, 5], as an image processing tool [11, 13, 19, 20].

Many efforts at finding a significant role for nonabelian group theory in DSP and image processing applications as well as in coding and communication theory have been limited by some or all of the following.

- The choice of an appropriate group or groups in a given application is not obvious.
- The lack of a large class of groups whose harmonic analysis is sufficiently understood for meaningful applications.
- The absence of a conceptual framework which relates group harmonic analysis to physically interpretable results.
- Fast algorithms may exist but are difficult to code as they do not easily lend themselves to modification.
- The lack of relevant models for applications which are not only a rephrasing of known methods or what is immediately available.

The language of group algebras over the complex field will be used throughout. Some readers may be more familiar with the identification of the group algebra $\mathbf{C}G$ with the space of all complex valued functions on G under G-convolution. Harmonic analysis over G usually includes a description of the (left) G-invariant and irreducible G-invariant subspaces and direct sum decompositions of $\mathbf{C}G$ into irreducible G-invariant subspaces.

For an abelian group A, complete answers to these problems can be given in terms of the characters of A. Moreover, these descriptions are especially simple. For example the irreducible A-invariant subspaces coincide with the one-dimensional subspaces spanned by the characters. The characters of A determine an orthogonal basis of $\mathbf{C}A$ and the finite Fourier transform relates the delta basis A of $\mathbf{C}A$ with the basis of characters of $\mathbf{C}A$. This is an extremely nice answer for applications since the characters of A can be physically interpreted as frequencies.

For finite groups $G = A \leftthreetimes B$, the semidirect product of normal abelian subgroup A with an abelian subgroup B, the characters of A and B play an equally important but more complicated role in the harmonic analysis of $A \leftthreetimes B$. We have developed harmonic analysis of such groups and directly linked this harmonic analysis to familiar DSP and image processing concepts. Moreover we have developed for groups $G = A \leftthreetimes B$

- algorithms for computing bases of irreducible G-invariant subspaces and bases compatible with direct sum decompositions of $\mathbf{C}G$ into G-invariant and irreducible G-invariant subspaces (spectral bases).
- fast algorithms for representing data, i.e., elements in $\mathbf{C}G$ over spectral bases.

- an extensive new class of fast unitary transforms for data analysis.

The direct sum decompositions of $\mathbf{C}G$ studied in this work are closely related to but are significantly different from those leading up to the Fourier transform of $\mathbf{C}G$ [10, 26]. Our decompositions are finer but are not generally uniquely determined.

We have extended our computational nonabelian group harmonic analysis technology to include semidirect products of the form $G = A \leftthreetimes H$, where A is an abelian group and $H = B \leftthreetimes C$ is the semidirect product of abelian groups B and C. In previous efforts, complete systems of primitive, pairwise orthogonal idempotents were built from characters of abelian groups. The current effort is based on

- adapting the Mackey-Wigner little group theorem to an algorithm for constructing such systems for general semidirect products $A \leftthreetimes H$, where A is abelian and H is arbitrary. This algorithm depends on knowing such systems for certain subgroups of H.

- extending the results on abelian group characters to general one-dimensional characters of nonabelian groups.

The complete algorithm computes systems of primitive, pairwise orthogonal idempotents for the groups G under study in terms of extensions of abelian group characters to one-dimensional characters of subgroups of G.

For a finite group G of the form $A \leftthreetimes (B \leftthreetimes C)$, where A, B and C are abelian groups, we have developed algorithms for constructing

- a complete primitive idempotent system in KG.

- a basis for each of the irreducible G-invariant subspaces generated by the primitive idempotents of the system.

- the expansion coefficients of $\alpha \in KG$ relative to the resulting basis of KG.

Algorithms for convolutions are investigated based on Wedderburn structure theorem. Compared to previous efforts, convolutions will be described in terms of two-sided G-invariant subspaces of $\mathbf{C}G$.

We have generalized the computational nonabelian group harmonic analysis technology by developing the theory and algorithms for abelian extensions. The previous efforts have been based on

- adapting the Mackey-Wigner (M-W) little group theorem to an algorithm for constructing such systems for general semidirect products $A \leftthreetimes H$, where A is abelian and H is arbitrary. This algorithm depends on knowing such systems for certain subgroups of H.

- extending the results on abelian group characters to general one-dimensional characters of nonabelian groups.

The complete algorithm computes systems of primitive, pairwise orthogonal idempotents for the groups G under study in terms of extensions of abelian group characters to one-dimensional characters of subgroups of G. A theorem of Wigner and Mackey provides a framework for constructing complete systems of primitive, pairwise orthogonal idempotents for semidirect product groups. However, M-W little group theorem requires knowledge of complete systems of primitive, pairwise orthogonal idempotents for certain subgroups of H even for semidirect product groups. The framework of abelian extensions simplifies algorithms, as well as includes groups not covered by the previous methods.

3 Mathematical Results

3.1 Introduction

From a mathematical perspective, a significant part of classical digital signal processing (DSP) can be viewed as topics in finite abelian group harmonic analysis [1, 6, 16, 4]. Fundamental DSP operations such as convolution and the Fourier transform can be identified with group algebra multiplication and group algebra direct sum decompositions into irreducible group invariant subspaces. This interplay, often implicit, has been responsible for fast algorithms such as the FFT [7], the use of FFT in computing large size convolutions and correlations, and more recently for the development of polynomial transforms [27, 25] for computing convolutions.

However pleasing, at least to the mathematically inclined, and useful this group theoretic approach to DSP, it is based on a seemingly magical relationship between DSP applications and finite abelian group harmonic analysis and the simplicity of this harmonic analysis. This magic can be explained by the powerful role played by abelian group characters in providing all that is required for finite abelian group harmonic analysis and the physical interpretation of these characters as frequency.

For some mathematicians, this group interpretation of DSP has raised the potential of an equally important application of nonabelian group harmonic analysis to DSP, especially in the construction of group transforms and group filters generalizing the classical Fourier transform and convolutional filters. The works of R. Holmes [14, 15], M. Karpovski and E. Trachtenberg [18] are the basis of much of the research in this direction. Similar ideas in coding theory have been introduced by F.J. MacWilliams [21]. These efforts have shown some promise but for the most part are more interesting to mathematicians than DSP engineers. A more successful application has been to fast algorithm design [2, 3, 10, 22, 23].

During the last ten years considerable effort has taken place to extend the success and range of applicability of nonabelian group methods to the design of new filters and spectral analysis methodologies [5, 8, 9], as an image processing tool [11, 13, 19, 20] and most recently as an image processing tool combined with graph theoretic modeling of image data [12, 24].

Many efforts at finding a significant role for nonabelian group theory in DSP and imaging applications as well as in coding and communication theory have been limited by some or all of the following.

- The choice of an appropriate group or groups in a given application is not obvious. Often the groups considered are those which are best known to the researcher.
- The lack of a large class of groups whose harmonic analysis is sufficiently understood for meaningful applications. Often the dihedral group with or without justification is the test example.
- The need to develop a conceptual framework which relates group harmonic analysis to physically interpretable results.
- Fast algorithms may exist but are difficult to code as they do not easily lend themselves to modification.

- Relevant models for applications which are not only a rephrasing of known methods or what is immediately available.

The finite nonabelian groups in this study have the form $G = A \leftthreetimes B$, the semidirect product of a normal abelian group A with an abelian group B. We will extend the results to finite groups $A \leftthreetimes H$, where H is an arbitrary group whose harmonic analysis is known. This includes finite groups of the form $A \leftthreetimes (B \leftthreetimes C)$, where A, B and C are abelian groups and in particular all crystallographic groups.

In the applications part, we will see how these nonabelian groups provide for new classes of imaging and DSP models.

The language of group algebras usually over the complex field will be used throughout. Some readers may be more familiar with the identification of the group algebra $\mathbf{C}G$ with the space of all complex valued functions on G under G-convolution. Harmonic analysis over G usually includes a description of the (left) G-invariant and irreducible G-invariant subspaces and direct sum decompositions of $\mathbf{C}G$ into irreducible G-invariant subspaces.

For an abelian group A, complete answers to these problems can be given in terms of the characters of A. Moreover, these descriptions are especially simple. For example the irreducible A-invariant subspaces coincide with the one-dimensional subspaces spanned by the characters. The characters of A determine an orthogonal basis of $\mathbf{C}A$ and the finite Fourier transform relates the delta basis A of $\mathbf{C}A$ with the basis of characters of A. This is an extremely nice answer for applications since the characters of A can be physically interpreted as frequencies.

For finite groups $A \leftthreetimes B$, the characters of A and B play an equally important but more complicated role in the harmonic analysis of $A \leftthreetimes B$. In this section, we will present the mathematical basis for $G = A \leftthreetimes B$ and extensions to $A \leftthreetimes (B \leftthreetimes C)$ and beyond for developing

- algorithms for computing bases of irreducible G-invariant subspaces and bases compatible with direct sum decompositions of $\mathbf{C}G$ into G-invariant and irreducible G-invariant subspaces (spectral bases).

- fast algorithms for representing data, i.e., elements in $\mathbf{C}G$ over spectral bases.

- an extensive new class of fast unitary transforms for data analysis.

We will have as a result *a large class of nonabelian groups with the potential of wide applicability to DSP and image processing whose harmonic analysis is known in detail. This harmonic analysis is based on abelian group characters which directly link this harmonic analysis to familiar DSP and imaging concepts.*

The direct sum decompositions of $\mathbf{C}G$ studied in this work are closely related to but are significantly different from those leading up to the Fourier transform of $\mathbf{C}G$ [10, 26]. Our decompositions are finer but are not generally uniquely determined.

Throughout this section, A and B denote finite abelian groups with composition given by multiplication. The identity is always denoted by 1 and the inverse of $x \in A$ by x^{-1}. The order of a set is the number of elements in the set.

For much of the general theory K denotes a field, finite or infinite, whose characteristic does not divide the orders of A and B. However for DSP and imaging applications, K is the field of complex numbers.

3.2 Abelian group A

3.2.1 Characters of Finite Abelian Groups

Suppose A is a finite abelian group of order N. A mapping $\tau : A \to \mathbf{C}^\times$ is called a *character* of A if τ is a homomorphism of the group A into the multiplicative group $\mathbf{C}^\times$ of nonzero elements in $\mathbf{C}$,

$$\tau(xy) = \tau(x)\tau(y), \quad x, y \in A.$$

Denote by A^* the set of all characters of A.

Denote by $U_N(\mathbf{C})$ the multiplicative group of all N-th roots of unity in $\mathbf{C}$. $U_N(\mathbf{C})$ is a cyclic subgroup of $\mathbf{C}^\times$ of order N. Since every $x \in A$ satisfies $x^N = 1$, $\tau(x) \in U_N(\mathbf{C})$, for every character τ of A.

In the following examples C_N is the cyclic group of order N having generator x.

Example 1 There exists N characters of C_N over $\mathbf{C}$ defined by

$$\tau_n(x) = e^{2\pi i \frac{n}{N}}, \quad 0 \le n < N.$$

Consider the direct product $C_{N_1} \times C_{N_2}$ of cyclic groups C_{N_1} and C_{N_2}. Denoting generators of C_{N_1} and C_{N_2} by x_1 and x_2, every element in $C_{N_1} \times C_{N_2}$ can be written uniquely in the form

$$x_1^{n_1} x_2^{n_2}, \quad 0 \le n_1 < N_1,\ 0 \le n_2 < N_2.$$

The characters of $C_{N_1} \times C_{N_2}$ are completely determined by the characters of C_{N_1} and C_{N_2}. If τ is a character of $C_{N_1} \times C_{N_2}$, we can define characters τ_1 and τ_2 of C_{N_1} and C_{N_2} by

$$\tau_1(x_1) = \tau(x), \quad \tau_2(x_2) = \tau(x_2).$$

τ is completely determined by τ_1 and τ_2 by

$$\tau(x_1^{n_1} x_2^{n_2}) = \tau_1(x_1)^{n_1} \tau_2(x_2)^{n_2}, \quad 0 \le n_1 < N_1,\ 0 \le n_2 < N_2,$$

and we can write $\tau = \tau_1 \otimes \tau_2$. Conversely, if τ_1 and τ_2 are characters of C_{N_1} and C_{N_2}, then $\tau_1 \otimes \tau_2$ is a character of $C_{N_1} \times C_{N_2}$.

Example 2 The $N_1 N_2$ characters

$$\tau_{\mathbf{n}}, \quad \mathbf{n} = (n_1, n_2),\ 0 \le n_1 < N_1,\ 0 \le n_2 < N_2,$$

of $C_{N_1} \times C_{N_2}$ are defined by

$$\tau_{\mathbf{n}}(x_1^{m_1} x_2^{m_2}) = e^{2\pi i \frac{n_1 m_1}{N_1}} e^{2\pi i \frac{n_2 m_2}{N_2}}, \quad 0 \le m_1 < N_1,\ 0 \le m_2 < N_2.$$

The results of this section easily extend to an arbitrary finite number of cyclic groups

$$A = C_{N_1} \times \cdots \times C_{N_R}.$$

Each character τ of A is uniquely represented by

$$\tau = \tau_1 \otimes \cdots \otimes \tau_R,$$

where τ_r is a character of C_{N_r}, $1 \leq r \leq R$. Since every finite abelian group A is the product of a finite number of finite cyclic groups, this completes the description of A^* for every finite abelian group A.

3.2.2 Group algebra of A

The group algebra $\mathbf{C}A$ of A over $\mathbf{C}$ is the $\mathbf{C}$-vector space of all formal sums

$$f = \sum_{x \in A} f(x)x, \quad f(x) \in \mathbf{C},$$

with $\mathbf{C}$-algebra multiplication

$$fg = \sum_{y \in A} \left(\sum_{x \in A} f(x)g(x^{-1}y) \right) y, \quad f, g \in \mathbf{C}A.$$

Denote by $L(A; \mathbf{C})$, the $\mathbf{C}$-vector space of all $\mathbf{C}$-valued functions on A. Every $f \in L(A : \mathbf{C})$ defines a formal sum in $\mathbf{C}A$

$$f = \sum_{x \in A} f(x)x$$

and we can identify the $\mathbf{C}$-vector space $\mathbf{C}A$ with the $\mathbf{C}$-vector space $L(A; \mathbf{C})$. The multiplication $f \cdot g$ in $\mathbf{C}A$ corresponds to the standard convolution in $L(A; \mathbf{C})$

$$f * g(y) = \sum_{x \in A} f(x)g(x^{-1}y), \quad y \in A,\ f, g \in L(A; \mathbf{C}).$$

Under this identification the delta function δ_y, $y \in A$ corresponds to the formal sum in $\mathbf{C}A$

$$\sum_{x \in A} \delta_y(x)x$$

which we denote by y. In this way, we can view A as a subset of $\mathbf{C}A$. A is a basis of the $\mathbf{C}$-vector space $\mathbf{C}A$ and $\mathbf{C}A$ has dimension N, the order of A. The identity 1 in A is the identity of the $\mathbf{C}$-algebra $\mathbf{C}A$.

We will usually use the term basis for any subset of vector space which if ordered is a basis in the usual sense. In summation expressions, there is no loss in doing so. However whenever matrices are involved, an ordering must be specified even if implicitly.

For $y \in A$ and $f \in \mathbf{C}A$

$$yf = \sum_{x \in A} f(x)yx = \sum_{x \in A} f(y^{-1}x)x.$$

We call yf the translation of f by y. The term $f(y^{-1}x)$ in the right-hand summation identifies yf with the usual definition of translation in engineering terminology. For $y \in A$, the operator $L(y)$ of $\mathbf{C}A$ defined by

$$L(y)f = yf, \quad f \in \mathbf{C}A,$$

is a linear isomorphism of the C-vector space $\mathbf{C}A$.

A subspace V of the C-vector space $\mathbf{C}A$ is called *A-invariant* if for each $y \in A$

$$yV = \{yf : f \in V\} \subset V.$$

For $g \in \mathbf{C}A$ define the operator $L(g)$ of $\mathbf{C}A$ by

$$L(g)f = gf, \quad f \in \mathbf{C}A.$$

Since

$$L(g)f = gf = \sum_{y \in A} g(y)(yf) = \sum_{y \in A} g(y)L(y)f = \left(\sum_{y \in A} g(y)L(y) \right) f$$

we have that

$$L(g) = \sum_{y \in A} g(y)L(y)$$

linearly extends the domain of definition of L from A to $\mathbf{C}A$. In particular, the two definitions coincide on A.

$L(g)$, $g \in \mathbf{C}A$, is a homomorphism of the C-vector space $\mathbf{C}A$ but is not necessarily an isomorphism as is the case with $L(y)$, $y \in A$. We can have $gf = 0$ for f, $g \in \mathbf{C}A$ with both f and g not zero.

For an A-invariant subspace V of $\mathbf{C}A$ and $f \in V$, we have for all $g \in \mathbf{C}A$,

$$L(g)f = \sum_{y \in A} g(y)L(y)f \in V$$

and V is $\mathbf{C}A$-invariant. The equivalence of A-invariance and $\mathbf{C}A$-invariance will be used throughout this work.

3.2.3 Fourier transform over A

Decompositions of $\mathbf{C}A$ into direct sums of A-invariant subspaces play two important roles: algorithm design for computing products in $\mathbf{C}A$ and spectral analysis. The Fourier transform over A is the simplest and most frequently occurring example.

A character τ of A determines the formal sum in $\mathbf{C}A$, $\tau = \sum_{x \in A} \tau(x)x$. Multiplication of characters will always be taken in $\mathbf{C}A$ with the warning that in many places, another multiplication is defined under which A^* is a group. The importance of characters in studying A-invariant subspaces of $\mathbf{C}A$ is contained in the following result.

Theorem 1 *For $f \in \mathbf{C}A$ and τ a character of A,*

$$f\tau = \hat{f}(\tau)\tau,$$

where $\hat{f}(\tau) \in \mathbf{C}$ is given by

$$\hat{f}(\tau) = \sum_{y \in A} f(y)\tau(y^{-1}).$$

Proof For $y \in A$

$$y\tau = \sum_{x \in A} \tau(x)yx = \sum_{x \in A} \tau(y^{-1}x)x = \tau(y^{-1}) \sum_{x \in A} \tau(x)x = \tau(y^{-1})\tau.$$

The theorem follows from

$$f\tau = \sum_{y \in A} f(y)(y\tau) = \left(\sum_{y \in A} f(y)\tau(y^{-1}) \right) \tau.$$

For two characters τ and λ of A, since $\tau\lambda = \lambda\tau$, we have

$$\tau\lambda = \alpha\lambda = \alpha\tau = \lambda\tau,$$

where $\alpha = \hat{\tau}(\lambda) = \hat{\lambda}(\tau)$. If $\tau \neq \lambda$, then $\alpha = 0$ and $\tau\lambda = 0$. If $\tau = \lambda$, then

$$\alpha = \sum_{y \in A} \tau(y)\tau(y^{-1}) = \sum_{y \in A} 1 = N$$

and $\tau^2 = N\tau$, proving the following.

Corollary 1 *For two characters τ and λ of A,*

$$\tau\lambda = \begin{cases} N\tau, & \tau = \lambda, \\ 0, & \tau \neq \lambda. \end{cases}$$

Corollary 2 *A^* is a linearly independent subset in the $\mathbf{C}$-vector space $\mathbf{C}A$.*

Proof Suppose

$$0 = \sum_{\tau \in A^*} \alpha(\tau)\tau, \quad \alpha(\tau) \in \mathbf{C}.$$

By corollary 1, for any $\lambda \in A^*$

$$\lambda \sum_{\tau \in A^*} \alpha(\tau)\tau = N\alpha(\lambda)\lambda = 0$$

and $\alpha(\lambda) = 0$. Since this holds for any $\lambda \in A^*$, the corollary follows.

By Theorem 1, the $\mathbf{C}$-subspace spanned by a character τ is A-invariant,

$$\mathbf{C}A\tau = \mathbf{C}\tau.$$

By corollary 2, we have the direct sum of one-dimensional A-invariant subspaces of $\mathbf{C}A$,

$$\sum_{\tau \in A^*} \oplus \mathbf{C}\tau.$$

3.2.4 Convolution theorem

By corollary 2, A^* is a basis of the C-vector space $\mathbf{C}A$ and we have the following result.

Theorem 2 $\mathbf{C}A$ *is the direct sum of one-dimensional* A*-invariant subspaces*

$$\mathbf{C}A = \sum_{\tau \in A^*} \oplus \mathbf{C}\tau.$$

By theorem 2,

$$1 = \sum_{\tau \in A^*} \alpha(\tau)\tau, \quad \alpha(\tau) \in \mathbf{C}.$$

For any $\lambda \in A^*$,

$$\lambda = \lambda \cdot 1 = \sum_{\tau \in A^*} \alpha(\tau)\lambda\tau = N\alpha(\lambda)\lambda$$

and $\alpha(\lambda) = \frac{1}{N}$, proving the following.

Corollary 3

$$1 = \frac{1}{N} \sum_{\tau \in A^*} \tau.$$

By corollary 3,

$$f = \frac{1}{N} \sum_{\tau \in A^*} f\tau = \frac{1}{N} \sum_{\tau \in A^*} \hat{f}(\tau)\tau$$

is the expansion of f over the basis A^* of $\mathbf{C}A$. The coefficient set of this expansion (up to scale multiple $\frac{1}{N}$)

$$\hat{f}(\tau), \quad \tau \in A^*,$$

is called the *Fourier transform* of f in $\mathbf{C}A$. By Theorem 1,

$$\hat{f}(\tau) = \sum_{y \in A} f(y)\tau(y^{-1}).$$

The basis A^* of $\mathbf{C}A$ is a *diagonalizing basis* for the operators $L(g)$, $g \in \mathbf{C}A$, since

$$L(g)\tau = g\tau = \hat{g}(\tau)\tau, \quad \tau \in A^*$$

and a diagonalizing basis for multiplication in $\mathbf{C}A$.

Theorem 3 *For* f *and* g *in* $\mathbf{C}A$,

$$fg = \frac{1}{N} \sum_{\tau \in A^*} \hat{f}(\tau)\hat{g}(\tau)\tau.$$

Proof

$$\begin{aligned} fg &= \frac{1}{N^2}\left(\sum_{\tau\in A^*}\hat{f}(\tau)\tau\right)\left(\sum_{\lambda\in A^*}\hat{g}(\lambda)\lambda\right) \\ &= \frac{1}{N^2}\sum_{\tau\in A^*}\sum_{\lambda\in A^*}\hat{f}(\tau)\hat{g}(\lambda)\tau\lambda \\ &= \frac{1}{N}\sum_{\tau\in A^*}\hat{f}(\tau)\hat{g}(\tau)\tau, \end{aligned}$$

completing the proof.

An A-invariant subspace W of $\mathbf{C}A$ is called *irreducible* if the only A-invariant subspaces of W are (0) and W. For $\tau \in A^*$, $\mathbf{C}\tau$ is an irreducible A-invariant subspace of $\mathbf{C}A$.

Theorem 4 *If W is an A-invariant subspace of $\mathbf{C}A$, then*

$$W = \sum_{\tau\in\Delta}\oplus\mathbf{C}\tau = \mathbf{C}Ae,$$

where $\Delta = W \cap A^*$ and $e = \frac{1}{N}\sum_{\tau\in\Delta}\tau$.

Proof For $f \in W$ and $\lambda \in A^*$

$$\lambda f = \frac{1}{N}\sum_{\tau\in A^*}\hat{f}(\tau)\lambda\tau = \frac{1}{N}\hat{f}(\lambda)\lambda.$$

Since W is A-invariant,

$$\hat{f}(\lambda)\lambda \in W, \quad \lambda \in A^*.$$

If $\hat{f}(\lambda) \neq 0$, then $\lambda \in W$ proving that every $f \in W$ is contained in the $\mathbf{C}$-linear span of the set of characters contained in W, proving $W = \sum_{\tau\in\Delta}\oplus\mathbf{C}\tau$.

Since $e \in W$ and W is A-invariant, $\mathbf{C}Ae \subset W$. For any $\lambda \in \Delta$, $\lambda e = \frac{1}{N}\lambda \in \mathbf{C}Ae$, proving $W \subset \mathbf{C}Ae$, completing the proof of the theorem.

The factor $\frac{1}{N}$ in the definition of e has been chosen so that $e^2 = e$, the relevance of which will be made clear in the next section.

If W is an irreducible A-invariant subspace of $\mathbf{C}A$, then by theorem 4, W contains a unique $\tau \in A^*$ and $W = \mathbf{C}\tau$, proving the following corollary.

Corollary 4 *The irreducible A-invariant subspaces of $\mathbf{C}A$ are given by $\mathbf{C}\tau$, $\tau \in A^*$.*

Denote the complement of $\Delta = W \cap A^*$ in A^* by Δ^c. By theorem 2 and theorem 4, we have the following result.

Corollary 5 *$\mathbf{C}A$ is the direct sum of A-invariant subspaces,*

$$\mathbf{C}A = W \oplus W',$$

where

$$W' = \sum_{\tau\in\Delta^c}\oplus\mathbf{C}\tau = \mathbf{C}Ae',$$

and $e' = \frac{1}{N}\sum_{\tau\in\Delta^c}\tau$.

3.3 Finite nonabelian group G

3.3.1 Group Algebras of Finite Group G

Suppose G is an arbitrary finite group of order N. The *group algebra* $\mathbf{C}G$ of G over $\mathbf{C}$ is the $\mathbf{C}$-vector space of all formal sums

$$f = \sum_{t \in G} f(t)t, \quad f(t) \in \mathbf{C},$$

with $\mathbf{C}$-algebra multiplication

$$fg = \sum_{t \in G} \left(\sum_{u \in G} f(u)g(u^{-1}t) \right) t, \quad f,\ g \in \mathbf{C}G.$$

Generally since G is not necessarily abelian, fg is not necessarily equal to gf, $f,\ g \in \mathbf{C}G$.

Denote by $L(G;\mathbf{C})$ the $\mathbf{C}$-vector space of all $\mathbf{C}$-valued functions on G. Every $f \in L(G;\mathbf{C})$ defines a formal sum in $\mathbf{C}G$, $f = \sum_{t \in G} f(t)t$ and we can identify the $\mathbf{C}$-vector space $\mathbf{C}G$ with the $\mathbf{C}$-vector space $L(G;\mathbf{C})$. The multiplication fg in $\mathbf{C}G$ corresponds to the possibly noncommutative convolution in $L(G;\mathbf{C})$

$$f * g(t) = \sum_{u \in G} f(u)g(u^{-1}t) = \sum_{u \in G} g(u)f(tu^{-1}), \quad f,\ g \in L(G;\mathbf{C}).$$

Under this identification the delta function δ_u, $u \in G$, corresponds to a formal sum having a single nonzero coefficient which we denote by u. In this way we can view G as a subset of $\mathbf{C}G$ and a basis of the $\mathbf{C}$-vector space $\mathbf{C}G$.

For $u \in G$ and $f \in \mathbf{C}G$,

$$uf = \sum_{t \in G} f(t)ut = \sum_{t \in G} f(u^{-1}t)t.$$

We call uf the *left translation* of f by u. Right translation can also be defined and generally differs from left translation, unless G is abelian. For $u \in G$, the operator $L(u)$ of $\mathbf{C}G$ defined by

$$L(u)f = uf, \quad f \in \mathbf{C}G,$$

is a linear isomorphism of the $\mathbf{C}$-vector space $\mathbf{C}G$.

A subspace V of the $\mathbf{C}$-vector space $\mathbf{C}G$ is called *G-invariant* if for all $u \in G$,

$$uV = \{uf : f \in V\} \subset V.$$

A G-invariant subspace V of $\mathbf{C}G$ is called *irreducible* if the only G-invariant subspaces of V are (0) and V. One of the main goals of nonabelian group harmonic analysis is to characterize the G-invariant, irreducible G-invariant and direct sum decompositions of $\mathbf{C}G$ into irreducible G-invariant subspaces. For an abelian group, its character theory provided all the necessary tools for answering these questions. Generally these problems require a vast mathematical machinery for their solution. However for the nonabelian groups considered

in this text, explicit solutions for many of these questions will be derived in terms of abelian group character theory.

For $g \in \mathbf{C}G$, the operator $L(g)$ of $\mathbf{C}G$ defined by

$$L(g)f = gf, \quad f \in \mathbf{C}G,$$

is a linear homomorphism of the $\mathbf{C}$-vector space $\mathbf{C}G$. Since

$$L(g) = \sum_{t \in G} g(t)L(t), \quad g \in \mathbf{C}G,$$

G-invariant subspace V of $\mathbf{C}G$ are $\mathbf{C}G$-invariant subspaces. If V is a G-invariant subspace of $\mathbf{C}G$ and $f \in V$, then for all $g \in \mathbf{C}G$, $gV \subset V$.

Idempotent theory provides a convenient language in which to express many of the results in the following chapters. However explicit results can usually be written in terms of abelian group character concepts.

A nonzero element $e \in \mathbf{C}G$ is called an *idempotent* if $e^2 = e$. Two idempotents e_1 and e_2 in $\mathbf{C}G$ are called *orthogonal* if $e_1e_2 = e_2e_1 = 0$. A set of pairwise orthogonal idempotents

$$\{e_j : 1 \leq j \leq J\}$$

is said to be *complete* if

$$1 = \sum_{j=1}^{J} e_j.$$

Example 3 If e is an idempotent in $\mathbf{C}G$, then $\{e, 1-e\}$ is a complete set of orthogonal idempotents.

Example 4 If e is an idempotent, then the G-invariant subspace generated by e, $\mathbf{C}Ge$, has e as a right unit

$$\mathbf{C}Ge = \{\alpha \in \mathbf{C}G : \alpha e = \alpha\}.$$

Example 5 If e is an idempotent then $\mathbf{C}G = \mathbf{C}Ge \oplus \mathbf{C}G(1-e)$.

The result described in example 5 holds generally for any complete set of orthogonal idempotents. We state the result without proof.

Theorem 5 *If*

$$\{e_j : 1 \leq j \leq J\}$$

is a complete set of orthogonal idempotents, then

$$\mathbf{C}G = \sum_{j=1}^{J} \oplus \mathbf{C}Ge_j.$$

Corollary 6 *If an idempotent e can be written as the sum of two orthogonal idempotents, $e = e_1 + e_2$, then*

$$\mathbf{C}Ge = \mathbf{C}Ge_1 \oplus \mathbf{C}Ge_2.$$

Example 6 If $\mathbf{C}G = W_1 \oplus W_2$, where W_1 and W_2 are G-invariant subspaces and

$$1 = e_1 + e_2, \quad e_1 \in W_1,\ e_2 \in W_2,$$

then $\{e_1, e_2\}$ is a complete set of orthogonal idempotents.

Generally we have the following result.

Theorem 6 *If $\mathbf{C}G$ is the direct sum of G-invariant subspaces, $\mathbf{C}G = \sum_{j=1}^{J} \oplus W_j$, and*

$$1 = \sum_{j=1}^{J} e_j, \quad e_j \in W_j,\ 1 \le j \le J,$$

then $\{e_j : 1 \le j \le J\}$ is a complete set of orthogonal idempotents.

Example 7 If $\mathbf{C}Ge = W_1 \oplus W_2$, the direct sum of G-invariant subspaces W_1 and W_2 with e an idempotent and $e = e_1 + e_2$, $e_1 \in W_1$, $e_2 \in W_2$, then e_1 and e_2 are orthogonal idempotents.

Theorem 7 *If $\mathbf{C}Ge$ is the direct sum of G-invariant subspaces*

$$\mathbf{C}Ge = \sum_{j=1}^{J} \oplus W_j,$$

with e an idempotent and

$$e = \sum_{j=1}^{J} e_j, \quad e_j \in W_j,\ 1 \le j \le J,$$

then $\{e_j : 1 \le j \le J\}$ is a set of pairwise orthogonal idempotents.

A homomorphism P of the $\mathbf{C}$-vector space $\mathbf{C}G$ is called a *projection* if $P^2 = P$. Every subspace W of $\mathbf{C}G$ determines a projection.

We will now show that every G-invariant subspace W of $\mathbf{C}G$ is generated by an idempotent. Consider any projection P of $\mathbf{C}G$ satisfying $W = \operatorname{im} P$ and define the mapping $P_0 : \mathbf{C}G \to \mathbf{C}G$ by

$$P_0(\alpha) = \frac{1}{N} \sum_{u \in G} u^{-1} P(u\alpha), \quad \alpha \in \mathbf{C}G.$$

P_0 is a homomorphism of the $\mathbf{C}$-vector space $\mathbf{C}G$. Since $P(u\alpha) \in W$, $u \in G$ and $\alpha \in \mathbf{C}G$, and W is G-invariant

$$P_0(\alpha) \in W, \quad \alpha \in \mathbf{C}G.$$

Theorem 8 *For all* $\alpha \in \mathbf{C}G$

$$P_0(\alpha) = \alpha P_0(1),$$

and if $\alpha \in W$, *then*

$$P_0(\alpha) = \alpha.$$

Proof For $t \in G$,

$$t^{-1}P_0(t) = \frac{1}{N}\sum_{u\in G} t^{-1}u^{-1}P(ut) = \frac{1}{N}\sum_{u\in G} u^{-1}P(u) = P_0(1),$$

by a change of variables. The linearity of P_0 proves the first part. If $\alpha \in W$, then $u\alpha \in W$, $u \in G$ and $P(u\alpha) = u\alpha$ implying

$$P_0(u\alpha) = \frac{1}{N}\sum_{u\in G} u^{-1}u\alpha = \alpha,$$

completing the proof.

Since $\operatorname{im} P_0 \subset W$ and P_0 acts by the identity mapping on W, by theorem 8 we have the following.

Corollary 7 P_0 *is a projection of* $\mathbf{C}G$ *satisfying* $W = \operatorname{im} P_0$.

Set $e = P_0(1)$.

Corollary 8 e *is a generating idempotent for* W,

$$W = \mathbf{C}Ge, \quad e^2 = e.$$

Since every G-invariant subspace W has a generating idempotent, by corollary 8, there exists a G-invariant subspace W' such that $\mathbf{C}G = W \oplus W'$. More generally we have the following result.

Corollary 9 *If* W_1 *and* W_2 *are* G*-invariant subspaces of* $\mathbf{C}G$ *such that* $W_1 \subset W_2$ *then there exists a* G*-invariant subspace* W_1' *of* W_2 *such that* $W_2 = W_1 \oplus W_1'$.

An idempotent $e \in \mathbf{C}G$ is called *primitive* if e can not be written as the sum of orthogonal idempotents in $\mathbf{C}G$.

Theorem 9 e *is a primitive idempotent in* $\mathbf{C}G$ *if and only if* $\mathbf{C}Ge$ *is irreducible.*

Proof If e is not primitive and $e = e_1 + e_2$, where e_1 and e_2 are orthogonal idempotents, then $\mathbf{C}G = \mathbf{C}Ge_1 \oplus \mathbf{C}Ge_2$ and $\mathbf{C}Ge$ is not irreducible. Conversely if W is a G-invariant subspace of $\mathbf{C}Ge$, then by corollary 9, $\mathbf{C}G = W \oplus W'$, for some G-invariant subspace W' of $\mathbf{C}Ge$. Example 7 implies e is not a primitive idempotent, completing the proof

The problem of constructing G-invariant, irreducible G-invariant and direct sum decompositions of $\mathbf{C}G$ into irreducible G-invariant subspaces can be replaced by that of constructing idempotents, primitive idempotents and complete sets of primitive orthogonal idempotents.

3.3.2 Group algebras of $A \leftthreetimes B$

A subgroup A of a group G is called *normal* if for all $t \in G$,

$$tAt^{-1} = \{tat^{-1} : a \in A\} \subset A.$$

G is said to be the *semidirect product* of a normal group A and a subgroup B if every $t \in G$ can be written uniquely as

$$t = xy, \quad x \in A,\ y \in B.$$

In this case we write $G = A \leftthreetimes B$.

For $\alpha \in \mathbf{C}A$ and $\beta \in \mathbf{C}B$, we can view $\alpha, \beta \in \mathbf{C}G$. If $\alpha\beta = 0$, then

$$\sum_{x\in A}\sum_{y\in B} \alpha(x)\beta(y)xy = 0$$

which implies

$$\alpha(x)\beta(y) = 0, \quad x \in A,\ y \in B,$$

and $\alpha = 0$ or $\beta = 0$.

Suppose $G = A \leftthreetimes B$ where A and B are abelian groups of orders L and M. Denote the character groups of A and B over $\mathbf{C}$ by A^* and B^*.

B acts on A^*. For $\tau \in A^*$ and $y \in B$ define $\tau^y \in \mathbf{C}G$ by

$$\tau^y = y\tau y^{-1}.$$

Since A is a normal subgroup of G

$$\tau^y = \sum_{x\in A} \tau(x)yxy^{-1} = \sum_{x\in A} \tau(y^{-1}xy)x$$

is also in A^*.

For $\tau \in A^*$

$$B\tau = \{\tau^y : y \in B\}$$

is a subset of A^* called the B-orbit over τ. A^* is partitioned into the disjoint union of distinct B-orbits.

Since

$$1 = \frac{1}{L}\sum_{\tau\in A^*} \tau, \quad 1 = \frac{1}{M}\sum_{\lambda\in B^*} \lambda,$$

we have

$$1 = \frac{1}{N}\sum_{\tau\in A^*}\sum_{\lambda\in B^*} \tau\lambda,$$

where $N = LM$ is the order of G. However generally τ and λ do not commute. We do have the following.

Theorem 10 *For $t = xy \in G$, $x \in A$, $y \in B$,*

$$t = \frac{1}{N}\sum_{\tau\in A^*}\sum_{\lambda\in B^*} \tau^y(x^{-1})\lambda(y^{-1})\tau^y\lambda.$$

Proof Since $x\tau^y = \tau^y(x^{-1})\tau^y$ and $y\lambda = \lambda(y^{-1})\lambda$,

$$t\tau\lambda = xy\tau\lambda = x\tau^y y\lambda = \tau^y(x^{-1})\lambda(y^{-1})\tau^y\lambda$$

completing the proof.

Since G is a basis of the $\mathbf{C}$-vector space $\mathbf{C}G$, by theorem 10, the collection of products in $\mathbf{C}G$

$$\{\tau\lambda : \tau \in A^*,\ \lambda \in B^*\}$$

is also a basis of $\mathbf{C}G$. Generally $\mathbf{C}G\tau\lambda$ is not one-dimensional, so that the spaces

$$\{\mathbf{C}G\tau\lambda : \tau \in A^*,\ \lambda \in B^*\}$$

intersect.

Generally to form direct sum decompositions of $\mathbf{C}G$ into left G-invariant subspaces we must modify the above approach. For $\tau \in A^*$, define

$$B(\tau) = \{y \in B : \tau^y = \tau\}.$$

$B(\tau)$ is a subgroup of B called the *centralizer* of τ in B.

Theorem 11 *If* $\tau_2 \in B\tau_1$, τ_1, $\tau_2 \in A^*$, *then*

$$B(\tau_1) = B(\tau_2).$$

We can assign a centralizer in B to every B-orbit in A^*. The assumption that B is abelian is essential.

Suppose $\tau \in A^*$ and consider $B(\tau)$. For $y \in B$, the set

$$yB(\tau) = \{yz : z \in B(\tau)\} \subset B$$

is called the left *coset* of $B(\tau)$ in B determined by y. The collection $B/B(\tau)$ of left cosets of $B(\tau)$ in B forms a partition of B. A set

$$\{y_s : 1 \le s \le S\} \subset B$$

is called a *complete system of representatives* of $B/B(\tau)$ if B is the disjoint union

$$B = \sum_{s=1}^{S} y_s B(\tau).$$

The B-orbit $B\tau$ has order S and $B\tau = \{\tau^{y_s} : 1 \le s \le S\}$. Generally the y_s, $1 \le s \le S$ depend on τ and when we need to express the dependence we write y_s^τ, $1 \le s \le S_\tau$. If M_τ denotes the order of $B(\tau)$,then $M = M_\tau S_\tau$, where M is the order of B.

We will now show that the collection of products

$$\frac{1}{L}\frac{1}{M_\tau}\tau\lambda, \quad \tau \in A^*,\ \lambda \in B(\tau)^*,$$

forms a complete set of primitive orthogonal idempotents for $\mathbf{C}G$. We break up the proof into the following three theorems.

Theorem 12 *For $\tau_1, \tau_2 \in A^*$ and $\lambda_1 \in B(\tau_1)^*$, $\lambda_2 \in B(\tau_2)^*$,*

$$(\tau_1\lambda_1)^2 = LM_{\tau_1}\tau_1\lambda_1$$

and

$$(\tau_1\lambda_1)(\tau_2\lambda_2) = 0, \text{ unless } \tau_1 = \tau_2 \text{ and } \lambda_1 = \lambda_2.$$

Proof Since $\tau_1^y = \tau_1$, $y \in B(\tau_1)$,

$$\tau_1\lambda_1 = \sum_{y\in B(\tau_1)} \lambda_1(y)\tau_1 y = \sum_{y\in B(\tau_1)} \lambda_1(y) y\tau_1 = \lambda_1\tau_1.$$

Consequently

$$(\tau_1\lambda_1)^2 = \lambda_1\tau_1^2\lambda_1 = L\tau_1\lambda_1^2 = LM_{\tau_1}\tau_1\lambda_1$$

and

$$(\tau_1\lambda_1)(\tau_2\lambda_2) = \lambda_1(\tau_1\tau_2)\lambda_2 = 0, \text{ unless } \tau_1 = \tau_2,$$

in which case

$$(\tau_1\lambda_1)(\tau_1\lambda_2) = \tau_1\lambda_1\lambda_2 = 0, \text{ unless } \lambda_1 = \lambda_2,$$

completing the proof.

By theorem 12, the collection of products is a set of orthogonal idempotents in $\mathbf{C}G$.

Theorem 13

$$1 = \sum_{\tau\in A^*} \sum_{\lambda\in B(\tau)^*} \frac{1}{L}\frac{1}{M_\tau}\tau\lambda.$$

Proof The theorem follows from

$$1 = \frac{1}{L}\sum_{\tau\in A^*} \tau$$

and

$$1 = \frac{1}{M_\tau}\sum_{\lambda\in B(\tau)^*} \lambda, \quad \tau \in A^*.$$

Theorem 13 implies completeness.

For $\tau \in A^*$ and $\lambda \in B(\tau)^*$, by theorem 12

$$e = \frac{1}{LM_\tau}\tau\lambda$$

is an idempotent. Since $\frac{1}{L}\tau$ is an idempotent and $\tau\lambda = \lambda\tau$

$$e = \frac{1}{L}\tau e = \frac{1}{L}e\tau.$$

Theorem 14 *If $\tau \in A^*$ and $\lambda \in B(\tau)^*$, then $e = \frac{1}{LM_\tau}\tau\lambda$ is a primitive idempotent.*

Proof Assume e is not primitive and $e = e_1 + e_2$ where e_1 and e_2 are orthogonal idempotents. Since

$$e_1 = e_1 e = \frac{1}{L} e_1 e\tau = \frac{1}{L} e_1 \tau$$

and

$$e_1 = e e_1 = \frac{1}{L}\tau e e_1 = \frac{1}{L}\tau e_1$$

we have

$$e_1 = e_1^2 = \frac{1}{L^2}\tau e_1^2 \tau = \frac{1}{L^2}\tau e_1 \tau.$$

Since A^* is a basis of $\mathbf{C}A$, we can write

$$e_1 = \frac{1}{L}\sum_{y\in B}\left(\sum_{\tau'\in A^*} e_1(\tau', y)\tau'\right) y, \quad e_1(\tau', y) \in \mathbf{C}.$$

Consequently

$$e_1 = \frac{1}{L^2}\tau e_1 \tau = \frac{1}{L^3}\sum_{y\in B}\sum_{\tau'\in A^*} e_1(\tau', y)\tau\tau' y\tau.$$

However

$$\tau\tau' y\tau = 0, \text{ unless } \tau' = \tau \text{ and } y \in B(\tau),$$

and

$$\tau^2 y\tau = L^2 \tau y, \quad y \in B(\tau),$$

implying

$$e_1 = \frac{1}{L}\tau \sum_{y\in B(\tau)} e_1(\tau, y) y = \frac{1}{L}\tau m_1, \quad m_1 \in \mathbf{C}B(\tau).$$

The same argument shows that

$$e_2 = \frac{1}{L}\tau m_2, \quad m_2 \in \mathbf{C}B(\tau),$$

implying

$$e = \frac{1}{LM_\tau}\tau\lambda = \frac{1}{L}\tau(m_1 + m_2).$$

Since $\tau \in \mathbf{C}A$ and λ, $m_1 + m_2 \in \mathbf{C}B(\tau)$,

$$\frac{1}{M_\tau}\lambda = m_1 + m_2.$$

We will show that m_1 and m_2 are orthogonal idempotents in $\mathbf{C}B(\tau)$, contradicting the fact that $\frac{1}{M_\tau}\lambda$ is a primitive idempotent in $\mathbf{C}B(\tau)$.

Since $\tau m_1 = m_1 \tau$,

$$e_1^2 = \frac{1}{L}\tau m_1^2 = \frac{1}{L}\tau m_1$$

implying $m_1^2 = m_1$. The same argument shows $m_2^2 = m_2$ and $m_1 m_2 = m_2 m_1 = 0$, completing the proof.

We have proved that the collection of products

$$\frac{1}{LM_\tau}\tau\lambda : \tau \in A^*,\ \lambda \in B(\tau)^*$$

is a complete set of primitive orthogonal idempotents for $\mathbf{C}G$ and we can apply the results of the previous chapter.

Theorem 15

$$\mathbf{C}G = \sum_{\tau \in A^*} \sum_{\lambda \in B(\tau)^*} \oplus \mathbf{C}G\tau\lambda$$

with the direct sum factors

$$\mathbf{C}G\tau\lambda, \quad \tau \in A^*,\ \lambda \in B(\tau)^*,$$

irreducible G-invariant subspaces of $\mathbf{C}G$.

If G is not abelian, an irreducible G-invariant subspace of $\mathbf{C}G$ is not necessarily one-dimensional. For groups of the form $G = A \leftthreetimes B$, with A and B abelian, we will determine bases for the subspaces $\mathbf{C}G\tau\lambda$, $\tau \in A^*$, $\lambda \in B(\tau)^*$, and derive fast algorithms for relating components in the G-basis to components in the new basis.

Suppose $\tau \in A^*$ and $\lambda \in B(\tau)^*$. Set $y_s = y_s^\tau$, $1 \le s \le S = S_\tau$ in the following discussion. For $x \in A$ and $y \in B$, with $y = y_s z$, $1 \le s \le S$ and $z \in B(\tau)$,

$$\begin{aligned} xy\tau\lambda &= xy_s z\tau\lambda = x\tau^{y_s} y_s z\lambda \\ &= \tau^{y_s}(x^{-1})\lambda(z^{-1})y_s\tau\lambda. \end{aligned}$$

Theorem 16 *For $\tau \in A^*$ and $\lambda \in B(\tau)^*$, the set*

$$\{y_s\tau\lambda : 1 \le s \le S\}$$

is a basis of the $\mathbf{C}$-vector space $\mathbf{C}G\tau\lambda$.

Proof Since the set

$$\{xy\tau\lambda : x \in A,\ y \in B\}$$

spans $\mathbf{C}G\tau\lambda$, the set

$$\{y_s\tau\lambda : 1 \le s \le S\}$$

spans $\mathbf{C}G\tau\lambda$. We must show that this set is linearly independent. Suppose that

$$0 = \sum_{s=1}^{S} \alpha(s) y_s\tau\lambda, \quad \alpha(s) \in \mathbf{C},\ 1 \le s \le S.$$

Multiplying on the left by τ^{y_t}, $1 \le t \le S$,

$$\begin{aligned} 0 = \tau_t^y 0 &= \sum_{s=1}^{S} \alpha(s) \tau^{y_t} \tau^{y_s} y_s \lambda \\ &= L\alpha(t) y_t \tau \lambda \end{aligned}$$

implying $\alpha(t) = 0$. Since t is arbitrary, $1 \le t \le S$, $\alpha(t) = 0$, for all $1 \le t \le S$, completing the proof.

For $\alpha \in \mathbf{C}G$,

$$\alpha = \frac{1}{L} \sum_{\tau \in A^*} \frac{1}{M_\tau} \sum_{\lambda \in B(\tau)^*} \alpha \tau \lambda$$

and by theorem 16

$$\frac{1}{L}\frac{1}{M_\tau} \alpha \tau \lambda = \sum_{s=1}^{S_\tau} \alpha_{\tau\lambda}(s) y_s^\tau \tau \lambda, \quad \alpha_{\tau\lambda}(s) \in \mathbf{C}.$$

Theorem 17 *For $\alpha \in \mathbf{C}G$, $\tau \in A^*$ and $\lambda \in B(\tau)^*$,*

$$\alpha_{\tau\lambda}(s) = \frac{1}{L}\frac{1}{M_\tau} \sum_{z \in B(\tau)} \left(\sum_{x \in A} \alpha(x y_s z) \tau^{y_s}(x^{-1}) \right) \lambda(z^{-1}),$$

where $y_s = y_s^\tau$, $1 \le s \le S$.

Proof Since

$$\alpha \tau \lambda = \sum_{s=1}^{S_\tau} \sum_{z \in B(\tau)} \sum_{x \in A} \alpha(x y_s z) x y_s z \tau \lambda,$$

the theorem follows from

$$x y_s z \tau \lambda = \tau^{y_s}(x^{-1}) \lambda(z^{-1}) y_s \tau \lambda, \quad z \in B(\tau),\ 1 \le s \le S_\tau.$$

3.3.3 Convolution Theorem

Decompositions of KG into direct sums of G-invariant subspaces

$$KG = \sum_{j=1}^{J} \oplus W_j$$

lead to block diagonal matrix representations of the left translation operators $L(\alpha)$, $\alpha \in KG$, and to fast algorithms for computing products in KG.

For $t \in G$, the matrix $P(t)$ of $L(t)$ relative to the basis G, of KG, ordered in some way, is a permutation matrix reflecting the group structure of G. The matrix $S(\alpha)$ of $L(\alpha)$, $\alpha \in KG$, relative to G is a linear combination over K of the permutation matrices $P(t)$, $t \in G$. If G is a cyclic group, then the corresponding matrices $P(t)$, $t \in G$, are cyclic shift matrices and the corresponding matrices $P(\alpha)$, $\alpha \in KG$, are circulant matrices. In this case the direct

sum decomposition of KG given by the characters diagonalizes the circulant matrices with the Fourier transform describing the change of basis.

Generally since W_j is G-invariant, $L(\alpha)$, $\alpha \in KG$, maps W_j into itself. Denoting by $T_j(\alpha)$ the matrix of the restriction of $L(\alpha)$ to some basis of W_j, the matrix direct sum

$$T(\alpha) = \sum_{j=1}^{J} T_j(\alpha),$$

is the matrix representation of $L(\alpha)$ relative to the basis of KG formed by piecing together the bases from the W_j, $1 \leq j \leq J$. We say the new basis is compatible with the direct sum decomposition of KG.

To compute

$$\alpha\beta = L(\alpha)\beta, \quad \alpha, \beta \in KG,$$

we write β in terms of the compatible basis, compute $T(\alpha)$ and form the matrix product of $T(\alpha)$ with the coordinates of β in the compatible basis and then translate the result back to the basis G.

In the following sections, we will carry out the program for the direct sum decomposition

$$KG = \sum_{\gamma \in A^*} \sum_{\lambda \in B(\tau)*} \oplus KG\tau\lambda,$$

relative to the idempotent basis

$$y_s^\tau \tau\lambda, \quad \tau \in A^*, \ \lambda \in B(\tau)^*, \ 1 \leq s \leq S_\tau.$$

Matrix Representation of L

For $\tau \in A^*$ and $\lambda \in B(\tau)^*$, denote by $L_{\tau\lambda}(g)$, $g \in KG$, the restriction of $L(g)$ to $KG\tau\lambda$ and by $T_{\tau\lambda}(g)$ the matrix of $L_{\tau\lambda}(g)$ relative to the idempotent basis of $KG\tau\lambda$. The matrix of $L(h)$ relative to the idempotent basis neglecting order) is given by the matrix direct sum

$$\sum_{\gamma \in A^*} \sum_{\lambda \in B(\tau)^*} T_{\tau\lambda}(g).$$

Right translation from A

Suppose $\tau \in A^*$ and $\lambda \in B(\tau)^*$. Set $y_s = y_s^\tau$, $1 \leq s \leq S = S_\tau$. For $x \in A$,

$$\begin{aligned} L_{\tau\lambda}(x)y)s\tau\lambda &= xy_s\tau\lambda \\ &= x\tau^{y_s}y_s\lambda \\ &= \tau^{y_s}(x^{-1})\tau^{y_s}y_s\tau \\ &= \tau^{y_s}(x^{-1})y_s\tau\lambda, \quad 1 \leq s \leq S, \end{aligned}$$

proving the following result.

Theorem 18 *For $\tau \in A^*$,*

$$T_{\tau\lambda}(x) = diag(\tau^{y_s}(x^{-1}))_{1\le s\le S}, hpp\lambda \in B(\tau)^*,\ x \in A,$$

with $y_s = y_s^\tau$, $1 \le s \le S = S_\tau$.

The diagonal matrix in the theorem depends solely on τ and is independent of λ leading to the following corollary.

Corollary 10 *For $\tau \in A^*$,*

$$\sum_{\lambda\in B(\tau)^* \oplus T_{\tau\lambda}(x)=I_{M_\tau}} \otimes diag\left(\tau^{y_s}(x^{-1})\right)_{1\le s\le S}, \quad x \in A,$$

with $y_s = y_s^\tau$, $1 \le s \le S = S_\tau$.

The corollary describes the matrix of the restriction of $L(x)$, $x \in A$, to the G-invariant subspaces $\sum_{\lambda\in B(\tau)^*} \oplus KG\tau\lambda$.

Corollary 11

$$T(x) = \sum_{\tau\in A^*} \oplus I_{M_\tau} \otimes diag\left(\tau^{y_s}(x^{-1})\right)_{1\le s\le S}, \quad x \in A,$$

where $\tau^{y_s} = t^{y_s^\tau}$, $1 \le s \le S = S_\tau$.

Left translation from B

The description of $T(t)$, $t \in B$, requires deeper analysis. For $\tau \in A^*$ and $\lambda \in B(\tau)^*$, we describe the matrix $T_{\tau\lambda}(t)$, $t \in B$, by the following steps.

- $T_{\tau\lambda}(y_s^\tau), \quad 1 \le s \le S_\tau.$
- $T_{\tau\lambda}\left(y_s^\tau B(\tau)\right), \quad 1 \le s \le S_\tau.$

Since B is the disjoint union

$$B = \cup_{1\le s\le S_\tau} y_s^\tau B(\tau)$$

all $T_{\tau\lambda}(t)$, $t \in B$, are described. The steps are dependent on $\tau \in A^*$.

Set $y_s = y_s^\tau$, $1 \le s \le S_\tau$. For $1 \le t \le S$,

$$y_t y_s = y_s' z, \quad 1 \le s, s' \le S,\ z \in B(\tau).$$

There exists a *permutation* $\pi_t^\tau \in Permm(S)$ such that

$$y_t y_s = y_{\pi_t^\tau}(s) z_t(s), \quad z_t(s) \in B(\tau),\ 1 \le s \le S.$$

For $1 \le t \le S$,

$$\begin{aligned} y_t y_s \tau\lambda &= y_{\pi_t^\tau(s)} z_t(s) \tau\lambda \\ &= y_{\pi_t^\tau(s)} \tau z_t(s)\lambda \end{aligned}$$

$$= \lambda(z_t(s)^{-1}) y_{\pi_t^\tau(s)} \tau\lambda, \quad 1 \le sS.$$

Denote by P_t^τ the $S \times S$ *permutation matrix* defined by

$$P_t^\tau = \left[e_{\pi_t(1)} \cdots e_{\pi_t(S)}\right], \quad 1 \le t \le S.$$

Theorem 19 *For $\tau \in A^*$ and $\lambda \in B(\tau)^*$,*

$$T_{\tau\lambda}(y_t^\tau) = P_t^\tau diag\left(\lambda(z_t(s))^{-1}\right)_{1\le s\le S_\tau}.$$

The permutation π_t^τ and the permutation matrix P_t^τ, $1 \le t \le S_\tau$, depend solely on $\tau \in A^*$ and are independent of $\lambda \in B(\tau)^*$, leading to the following corollary.

Corollary 12 *For $\tau \in A^*$,*

$$\sum_{\lambda\in B(\tau)^*} \oplus T_{\tau\lambda}(y_t^\tau) = (I_{M_\tau} \otimes P_t^\tau) \sum_{\lambda\in B(\tau)^*} diag\left(\lambda((z_t(s))^{-1}\right)_{1\le s\le S_\tau}.$$

By the corollary, the matrix of the restriction of $L(y_t^\tau)$ to the G-invariant subspace

$$\sum_{\lambda\in B(\tau)^*} \oplus KG\tau\lambda$$

uses the same permutation matrix P_t^τ on each $KG\tau\lambda$, $\lambda \in B(\tau)^*$. This step requires for each $\tau \in A^*$, S_τ permutation matrices P_t^τ, $1 \le t \le S_\tau$.

Suppose there exists $y = y^\tau \in B$ such that

$$y^s, \quad 0 \le s < S = S_\tau$$

is a complete system of left coset representatives of $B/B(\tau)$. The idempotent basis of $KG\tau\lambda$ is given by

$$y^s\tau\lambda, \quad 0 \le s < S.$$

For $0 \le t < S$,

$$y^t y^s \tau\lambda = y^{t+s}\tau\lambda,$$

where $t + s$ is taken modulo S. We now have

$$T_{\tau\lambda}(y^t) = P^t,$$

where P is the S-point cyclic shift matrix

$$P = \begin{bmatrix} 0 & \cdot & \cdot & \cdot & 0 & 1 \\ 1 & & & & & \\ 0 & 1 & & & & \\ \cdot & & \cdot & & & \\ \cdot & & & \cdot & & \\ 0 & & & & 1 & 0 \end{bmatrix}.$$

For $z \in B(\tau)$,

$$zy_s\tau\lambda = \lambda(z^{-1})y_s\tau\lambda, \quad 1 \le s < S,$$

implying that $T_{\tau\lambda}(z)$ is the *scalar* matrix

$$T_{\tau\lambda}(z) = \lambda(z^{-1})I_{S_\tau}, \quad z \in B(\tau).$$

Theorem 20 *For $\tau \in A^*$ and $\lambda \in B(\tau)^*$,*

$$T_{\tau\lambda}(y_t z) = \lambda(z^{-1}) P_t^\tau diag\left(\lambda((z_t(s))^{-1}\right)_{1\le s\le S_\tau},$$

with $1 \le t \le S_\tau$ and $z \in B(\tau)$.

Corollary 13

$$\sum_{\lambda\in B(\tau)^*} \oplus T_{\tau\lambda}(y_t z) = (I_{M_\tau} \otimes P_t^\tau) \sum_{\lambda\in B(\tau)^*} \lambda(z^{-1}) diag\left(\lambda((z_t(s))^{-1}\right)_{1\le s\le S_\tau}.$$

3.4 Characters of Nonabelian Groups

Assume throughout that the characteristic of K is relatively prime to the order $|G|$ of G.

3.4.1 Basic Properties

A mapping $\rho : G \longrightarrow K^\times$ is called a *one-dimensional character* of G over K if ρ is a group homomorphism,

$$\rho(xy) = \rho(x)\rho(y), \text{ whenever } x, y \in G. \tag{1}$$

One-dimensional characters of nonabelian groups share with abelian group characters the property that they generate one-dimensional G-invariant subspaces. Since we will not use the more general concept of a character of a group representation of G, we will use the term character to mean one-dimensional character.

As a function on G, a character ρ of G can be viewed as an element in KG,

$$\rho = \sum_{x\in G} \rho(x)x.$$

Several of the proofs below are exactly the same as in the abelian case, but we include them for completeness.

Theorem 21 *Suppose ρ is a character of G. For any $t \in G$ and $\alpha \in KG$,*

$$t\rho = \rho t = \rho(t^{-1})\rho$$

and

$$\alpha\rho = \rho\alpha = \widehat{\alpha}(\rho)\rho,$$

where

$$\widehat{\alpha}(\rho) = \sum_{t\in G} \alpha(t)\rho(t^{-1}).$$

Proof From (1) and changing variables, we have

$$t\rho = \sum_{x\in G} \rho(x)tx = \sum_{x\in G} \rho(t^{-1}x)x = \rho(t^{-1}) \sum_{x\in G} \rho(x)x = \rho(t^{-1})\rho,$$

and

$$\rho t = \sum_{x\in G} \rho(x)xt = \sum_{x\in G} \rho(xt^{-1})x = \rho(t^{-1}) \sum_{x\in G} \rho(x)x = \rho(t^{-1})\rho,$$

proving the first statement.

Using the first statement, we have

$$\alpha\rho = \sum_{t\in G} \alpha(t)t\rho = \left(\sum_{t\in G} \alpha(t)\rho(t^{-1})\right)\rho,$$

and

$$\rho\alpha = \sum_{t\in G} \alpha(t)\rho t = \left(\sum_{t\in G} \alpha(t)\rho(t^{-1})\right)\rho,$$

completing the proof.

For $\gamma \in KG$, define the *centralizer* $G(\gamma)$ of γ in G by

$$G(\gamma) = \{t \in G : t\gamma = \gamma t\}.$$

$G(\gamma)$ is a subgroup of G. The *center* of KG is the set of all $\gamma \in KG$ such that $G = G(\gamma)$. γ is in the center of KG if and only if we have $\gamma\alpha = \alpha\gamma$, for all $\alpha \in KG$. By Theorem 10, every character ρ of G is in the center of KG.

Characters of G generate one-dimensional G-invariant subspaces. For a character ρ of G,

$$KG\rho = \{\hat{\alpha}(\rho)\rho : \alpha \in KG\}. \tag{2}$$

In fact we have the following.

Theorem 22 *Every one-dimensional G-invariant subspace of KG is generated by a character of G over K.*

Proof Suppose $KG\gamma$, $\gamma \in KG$, is one-dimensional. For $t \in G$,

$$t\gamma = \alpha(t)\gamma, \quad \alpha(t) \in K^{\times}.$$

Without loss of generality, we can assume $\gamma(1) = 1$. Since $(st)\gamma = s(t\gamma)$, we have $\alpha(st) = \alpha(s)\alpha(t)$, for all s, $t \in G$. α and γ are then characters of G over K, completing the proof.

Denote by G^* the collection of all characters of G over K.

Theorem 23 *For characters ρ_1 and ρ_2 of G over K, if $\rho_1 \neq \rho_2$, then*

$$\rho_1^2 = |G|\rho_1$$

and

$$\rho_1\rho_2 = \rho_2\rho_1 = 0.$$

Proof Since $\rho_1^2 = \widehat{\rho}_1(\rho_1)\rho_1$, we have by (1),

$$\widehat{\rho}_1(\rho_1) = \sum_{t\in G} \rho_1(t)\rho_1(t^{-1}) = \sum_{t\in G} \rho_1(1) = |G|,$$

the first result follows.

If $\rho_1 \neq \rho_2$, $\widehat{\rho}_2(\rho_1) = \widehat{\rho}_1(\rho_2)$ and

$$\rho_1\rho_2 = \widehat{\rho}_2(\rho_1)\rho_1 = \widehat{\rho}_1(\rho_2)\rho_2$$

imply $\rho_1\rho_2 = 0$, completing the proof.

As a consequence of the theorem, if ρ_1 and ρ_2 are distinct characters of G over K,

$$\widehat{\rho}_1(\rho_2) = \sum_{t\in G} \rho_1(t)\rho_2(t^{-1}) = 0.$$

By Theorem 13, we have the following.

Corollary 14 *The collection*

$$\left\{\frac{1}{|G|}\rho : \rho \in G^*\right\}$$

is a system of primitive pairwise orthogonal idempotents in KG.

The corollary implies G^* is linearly independent.

For a finite nonabelian group G, KG cannot decompose into the direct sum of one-dimensional G-invariant subspaces, since this would imply that G is isomorphic to a group of diagonal matrices which is clearly an abelian group. Unlike the finite abelian group case splitting over K, the collection in Corollary (14) is not complete. However a complete system of orthogonal primitive idempotents in KG exists. Necessarily some of these idempotents are not characters of G and generate G-invariant subspaces of dimension greater than one. In the following section, for the classes of groups considered, we will compute such systems. We will lay the foundation for doing so by first establishing additional properties of characters of G and characters of subgroups of G.

For $y \in G$ and $\alpha \in KG$, define $\alpha^y \in KG$ by

$$\alpha^y = y\alpha y^{-1} = \sum_{x\in G} \alpha(y^{-1}xy)x. \tag{3}$$

The mapping of KG defined by (3) is an automorphism of the group algebra KG. By Theorem 10, if ρ is a character of G then for all $y \in G$, $\rho^y = \rho$.

A subgroup H of G is called *normal* if for all $y \in G$,

$$yHy^{-1} = \{yxy^{-1} : x \in H\} \subset H.$$

If $\alpha \in KH$,

$$\alpha = \sum_{x \in H} \alpha(x)x$$

and $y \in G$ then since $yxy^{-1} \in H$, for all $x \in H$,

$$\alpha^y = \sum_{x \in H} \alpha(x)yxy^{-1} = \sum_{x \in H} \alpha(y^{-1}xy)x$$

is again in KH. The automorphism (3) maps KH onto itself, for every $y \in G$.

Suppose throughout that H *is a normal subgroup of* G. For a character ρ of H we have, for every $y \in G$, that ρ^y is a character of H, i.e., the mapping

$$x \longrightarrow \rho(y^{-1}xy), \quad x \in H,$$

is a character of H. In this way G acts on H^*, the collection of characters of H over K. This action plays a major role throughout this work. We will introduce certain constructions associated to this action at this time and leave to later sections their application.

Consider $\rho \in H^*$ and define

$$G^\rho = \{\rho^y : y \in G\}.$$

G^ρ is a subset of H^* called the *G-orbit* over ρ. Two G-orbits which intersect must be equal. As a result, H^* is the disjoint union of its distinct G-orbits. A subset of H^*,

$$\{\rho_1, \ldots, \rho_R\}$$

is called a *complete set of representatives* for the G-orbits in H^* if H^* is the disjoint union

$$H^* = \cup_{r=1}^{R} G^{\rho_r}.$$

For $\rho \in H^*$, the *centralizer* of $\rho \in G$,

$$G(\rho) = \{y \in G : \rho^y = \rho\}$$

is a subgroup of G containing H.

Theorem 24 *For $\rho \in H^*$ and $y \in G$, we have*

$$G(\rho^y) = yG(\rho)y^{-1}.$$

Proof If $z \in G(\rho)$ then since

$$\begin{aligned}(yzy^{-1})\rho^y &= yzy^{-1}y\rho y^{-1} = yz\rho y^{-1} = y\rho zy^{-1} \\ &= y\rho y^{-1}yzy^{-1} = \rho^y(yzy^{-1}),\end{aligned}$$

we have $yzy^{-1} \in G(\rho^y)$. A similar argument shows that $u \in G(\rho^y)$ implies $y^{-1}uy \in G(\rho)$, completing the proof.

In general, $G(\rho)$ is not a normal subgroup of G. However, if it is, we have the following corollary.

Corollary 15 *If $\rho \in H^*$ and $G(\rho)$ is a normal subgroup of G, then for all $z \in G$, $G(\rho^z) = G(\rho)$.*

Some more group theory is necessary for the next set of results. For $y \in G$, the subset of G,

$$Hy = \{zy : z \in H\}$$

is called a *left H-coset over y*. Left H-cosets which intersect are equal and so G is the disjoint union of its distinct left H-cosets. Since H is a normal subgroup of G, a group multiplication can be placed on the collection of left H-cosets by

$$(Hy_1)(Hy_2) = H(y_1y_2), \quad y_1,\ y_2 \in G.$$

Normality is used to show that the multiplication is well defined in the sense that if $Hy_1 = Hy_1'$ and $Hy_2 = Hy_2'$ then $H(y_1y_2) = H(y_1'y_2')$, $y_1',\ y_2' \in G$. The resulting group is denoted by $H\backslash G$. H is the identity element and Hy^{-1} is the inverse of Hy in $H\backslash G$.

A subset of G

$$\{y_r : 0 \le r < R\}, \tag{4}$$

is called a *complete set of representatives for $H\backslash G$* if G is the disjoint union of the left-cosets over y_r, $0 \le r < R$. We will always take $y_0 = 1$ in G.

3.4.2 Primitive Idempotents

A character ρ of H over K determines the primitive idempotent $\frac{1}{|H|}\rho$ in KH. However, in general, $\frac{1}{|H|}\rho$ is not a primitive idempotent in KG. We continue assuming that H is a normal subgroup of G.

Theorem 25 *Suppose $\rho \in H^*$ and set $f = \frac{1}{|H|}\rho$. If*

$$f = e_1 + e_2,$$

where e_1 and e_2 are orthogonal idempotents in KG, then e_1 and e_2 are in the $KG(\rho)$.

Proof Since e_1 and e_2 are orthogonal idempotents,

$$fe_1 = e_1^2 + e_2e_1 = e_1 = e_1^2 + e_1e_2 = e_1f.$$

From (4), we can write

$$e_1 = \sum_{r=0}^{R-1} \sum_{x \in H} e_1(xy_r)xy_r.$$

Theorem·10 implies

$$\begin{aligned} e_1 &= fe_1 = \frac{1}{|H|} \sum_{r=0}^{R-1} \sum_{x \in H} e_1(xy_r)(\rho x)y_r \\ &= f \sum_{r=0}^{R-1} \left(\sum_{x \in H} e_1(xy_r)\rho(x^{-1}) \right) y_r = f \sum_{r=0}^{R-1} \alpha_1(r)y_r, \quad \alpha_1(r) \in K. \end{aligned}$$

Since

$$e_1 = e_1f = \frac{1}{|H|^2} \sum_{r=0}^{R-1} \alpha(r)\rho\rho^{y_r}y_r$$

we have from Theorem 13, that

$$e_1 = f \sum_{y_r \in G(\rho)} \alpha(r)y_r,$$

which since $H \subset G(\rho)$ implies $e_1 \in KG(\rho)$. The same argument shows that $e_2 \in KG(\rho)$, completing the proof.

Normality of H in G is essential since it is required for $y_r\rho y_r^{-1} \in H^*$ and

$$\rho y_r \rho y_r^{-1} = 0$$

unless $y_r \in G(\rho)$.

Corollary 16 *If $\rho \in H^*$ and $H = G(\rho)$ then $\frac{1}{|H|}\rho$ is a primitive idempotent in KG.*

Theorem 25 and Corollary 16 motivate a strategy for constructing primitive idempotents in KG. For the groups considered in the following two sections this strategy will lead to algorithms for constructing complete system of primitive pairwise orthogonal idempotents in KG. We begin with a character ρ of H over K and search for extensions of ρ to characters ρ_1 over subgroups H_1 in G containing H with the hope that $H_1 = G(\rho_1)$.

Assume throughout that *H is a normal subgroup of G such that the group of left H-cosets $H\backslash G$ is an abelian group.* Under this assumption any subgroup H_1 of G containing H is a normal subgroup of G.

Suppose H_1 is a subgroup of G containing H. Since H is the identity element in the group $H\backslash G$, for all $x_1, x_2 \in G$, the *commutator*

$$x_1x_2x_1^{-1}x_2^{-1} \in H.$$

If $x_2 \in H_1$, then

$$x_1 x_2 x_1^{-1} \in Hx_2 \subset H_1, \quad x_1 \in G,$$

proving H_1 is a normal subgroup of G.

Suppose ρ is a character of H over K. A subgroup H_1 of G *admits an extension* of ρ if $H \subset H_1$ and there exists a character ρ_1 of H_1 over K extending ρ,

$$\rho_1(x) = \rho(x), \quad x \in H.$$

We say simply that ρ_1 is an *extension* of ρ to H_1.

Theorem 26 *If H_1 admits an extension of ρ then $H_1 \subset G(\rho)$.*

Proof Suppose ρ_1 is an extension of ρ to H_1. For $x \in H$ and $y \in H_1$,

$$\rho_1(yx) = \rho_1(y)\rho(x)$$

and since $yxy^{-1} \in H$,

$$\rho_1(yx) = \rho_1(yxy^{-1}y) = \rho(yxy^{-1})\rho_1(y) = \rho^y(x)\rho_1(y).$$

As a result

$$\rho(x) = \rho^y(x), \quad x \in H,\ y \in H_1,$$

proving the theorem.

Theorem 27 *Suppose H_1 admits an extension of ρ. If ρ_1 and ρ_2 are two extensions of ρ to H_1, then*

$$H_1 \subset G(\rho_1) = G(\rho_2) \subset G(\rho).$$

Proof For $y \in G(\rho_1)$ and $c \in H_1$,

$$\rho_1(yxy^{-1}x^{-1}) = \rho_1^y(x)\rho_1(x^{-1}) = 1.$$

Since $yxy^{-1}x^{-1} \in H$,

$$\rho(yxy^{-1}x^{-1}) = 1.$$

Writing

$$\begin{aligned} \rho_2(yxy^{-1}) &= \rho_2(yxy^{-1}x^{-1}x) = \rho(yxy^{-1}x^{-1})\rho_2(x) \\ &= \rho_2(x), \end{aligned}$$

we have $G(\rho_1) \subset G(\rho_2)$. The same argument shows $G(\rho_2) \subset G(\rho_1)$, proving $G(\rho_1) = G(\rho_2)$.

If we take $x \in H$, then yxy^{-1} and x^{-1} are in H and

$$\rho(yxy^{-1}x^{-1}) = \rho^y(x)\rho(x^{-1}), \quad x \in H,$$

implying $G(\rho_1) \subset G(\rho)$ and completing the proof.

Suppose H_1 admits an extension ρ_1 of ρ. Denote by $\rho(H_1)$ the collection of all extensions of ρ to H_1. We can construct $\rho(H_1)$ from ρ_1 and $(H\backslash H_1)^*$ the collection of all characters of the finite abelian group $H\backslash H_1$ over K.

For $\tilde{\chi} \in (H\backslash H_1)^*$, the mapping $\chi : H_1 \longrightarrow K$, defined by

$$\chi(x) = \tilde{\chi}(Hx), \quad x \in H_1,$$

is an extension of the trivial character on H to H_1,

$$\chi(x) = 1, \text{ for all } x \in H.$$

We can identify $(H\backslash H_1)^*$ with the collection of all extensions of the trivial character on H to H_1.

Suppose ρ_1 is an extension of ρ to H_1. For any $\tilde{\chi} \in (H\backslash H_1)^*$, the mapping $\rho_1^{\chi} : H_1 \longrightarrow K^{\times}$, defined by

$$\rho_1^{\chi}(x) = \chi(x)\rho_1(x), \quad x \in H_1,$$

is an extension of ρ to H_1. Conversely if ρ_2 is any extension of ρ to H_1 then

$$\chi(x) = \rho_1(x)\rho_2(x^{-1}), \quad x \in H_1,$$

is an extension of the trivial character on H to H_1, proving the following result.

Theorem 28 *Suppose ρ_1 is an extension of ρ to H_1. Then*

$$\rho(H_1) = \{\rho_1^{\chi} : \tilde{\chi} \in (H\backslash H_1)^*\}.$$

Every extension of ρ to H_1 has a unique representation of the form

$$\rho_1^{\chi}, \quad \tilde{\chi} \in (H\backslash H_1)^*.$$

In particular, the order of $\rho(H_1)$ is the order of $(H\backslash H_1)^*$. If $H\backslash H_1$ splits over K, the order is the order of $H\backslash H_1$.

We will use Theorem 28 to prove a result which is essential for establishing completeness of certain systems of primitive pairwise orthogonal idempotents.

Theorem 29 *Suppose H_1 admits an extension of ρ and $H\backslash H_1$ splits over K. Then*

$$\frac{1}{|H|}\rho = \frac{1}{|H_1|} \sum_{\rho_1 \in \rho(H)} \rho_1.$$

Proof Suppose ρ_1' is an extension of ρ to H_1. By Theorem 28, for any $x \in H_1$,

$$\sum_{\rho_1 \in \rho(H_1)} \rho_1(x) = \rho_1'(x) \sum_{\tilde{\chi} \in (H \backslash H_1)^*} \tilde{\chi}(Hx).$$

The righthand summation vanishes unless $x \in H$ and we have for $x \in H$,

$$\sum_{\rho_1 \in \rho(H_1)} \rho_1(x) = \rho(x) \frac{|H_1|}{|H|},$$

completing the proof.

Suppose H_1 admits an extension ρ_1 of ρ. Choose a complete set of representatives

$$\{y_r : 0 \leq r < R\}$$

for the group $H \backslash H_1$. Every $y \in H_1$ has a unique representation of the form $y = xy_r$, $x \in H$, $0 \leq r < R$. We can write

$$\rho_1 = \sum_{r=0}^{R-1} \sum_{x \in H} \rho_1(xy_r) x y_r = \sum_{x \in H} \rho(x) x \sum_{r=0}^{R-1} \rho_1(y_r) y_r$$

and we have

$$\rho_1 = \rho \sum_{r=0}^{R-1} \rho_1(y_r) y_r.$$

In particular, if ρ' is a character of H over K and $\rho' \neq \rho$, then $\rho' \rho_1 = \rho_1 \rho' = 0$. This result has the following important consequence.

Theorem 30 *For distinct characters ρ and ρ' of H over K and extensions ρ_1 and ρ_1' to H_1 and H_1' we have $\rho_1 \rho_1' = \rho_1' \rho_1 = 0$.*

By Theorem 26 and the corollary to Theorem ??, if $H = G(\rho)$ then ρ cannot be extended and $\frac{1}{|H|}\rho$ is a primitive idempotent in KG. Explicit algorithm for constructing primitive idempotents is presented in Subsection 4.1.1.

3.5 A Theorem of Mackey and Wigner

Suppose G is a finite group having the form $G = A \leftthreetimes H$ where A is an abelian group of order $|A|$ splitting over the field K and H is an arbitrary subgroup. The main result in this section is a theorem due to Wigner and Mackey. The result provides a framework for constructing complete systems of primitive, pairwise orthogonal idempotents for semidirect product groups. The construction of such systems in the preceding section can be viewed as a special, simple case.

The Mackey-Wigner (M-W) little group theorem is not the end of the story even for semidirect product groups since it requires knowledge of complete systems of primitive, pairwise orthogonal idempotents for certain subgroups of H. In the preceding section, H is abelian and such systems are given in terms of abelian group character theory. We will use the M-W theorem, along with the results of section 3.4, to find such systems for KG, where H has the form $H = B \leftthreetimes C$, with B and C abelian groups.

3.5.1 M-W Theorem

Suppose for $\tau \in A^*$,

$$\{f_\tau^\tau : 1 \le r \le r_\tau\}$$

is a complete system of primitive, pairwise orthogonal idempotents for $KH(\tau)$. *Then the set of products*

$$\frac{1}{|A|}\tau f_\tau^\tau, \quad \tau \in A^*,\ 1 \le r \le r_\tau, \tag{5}$$

is a complete system of primitive, pairwise orthogonal idempotents for KG.

Theorem 31 *Suppose* $\tau \in A^*$ *and* $\alpha \in KG$ *satisfies*

$$\frac{1}{|A|}\tau\alpha = \alpha = \alpha\left(\frac{1}{|A|}\tau\right).$$

Then $\alpha = \frac{1}{|A|}\tau m$, $m \in KH(\tau)$.

Proof Write

$$\alpha = \sum_{y\in H}\sum_{x\in A}\alpha(xy)xy.$$

Since $\alpha = \frac{1}{|A|}\tau\alpha$, we have

$$\alpha = \frac{1}{|A|}\sum_{y\in h}\left(\sum_{x\in A}\alpha(xy)\tau x\right)y = \frac{1}{|A|}\tau\sum_{y\in H}\left(\sum_{x\in A}\alpha(xy)\tau(y^{-1})\right)y,$$

which we write as

$$\alpha = \frac{1}{|A|}\tau\sum_{y\in H}\tilde{\alpha}(y)y, \quad \tilde{\alpha}(y) \in K.$$

Since $\alpha = \alpha\left(\frac{1}{|A|}\tau\right)$, we have

$$\alpha = \frac{1}{|A|^2}\sum_{y\in H}\tilde{\alpha}(y)\tau\tau^y y.$$

$\tau\tau^y = 0$, unless $y \in H(\tau)$, implies

$$\alpha = \frac{1}{|A|}\tau\sum_{y\in H(\tau)}\tilde{\alpha}(y)y = \frac{1}{|A|}\tau m, \quad m \in KH(\tau),$$

completing the proof.

In the following, we will several times use the result that if $\alpha \in KA$ and $\beta \in KH$, the $\alpha\beta = 0$, if and only if $\alpha = 0$ or $\beta = 0$.

Theorem 32 *Suppose* $\tau \in A^*$ *and* f *is a primitive idempotent in* $KH(\tau)$. *Then* $e = \frac{1}{|A|}\tau f$ *is a primitive idempotent in* KG.

Proof τ and f commute, implying e is an idempotent. Suppose e is not primitive and we can write $e = e_1 + e_2$, where e_1 and e_2 are orthogonal idempotents in KG. Since $\frac{1}{|A|}\tau e = e = e\left(\frac{1}{|A|}\tau\right)$ and $ee_1 = e_1 = e_1 e$, we have

$$\frac{1}{|A|}\tau e_1 = e_1 = e_1\left(\frac{1}{|A|}\tau\right).$$

Applying Theorem 31,

$$e_1 = \frac{1}{|A|}\tau m_1, \quad m_1 \in KH(\tau).$$

In the same way $e_2 = \frac{1}{|A|}\tau m_2$, $m_2 \in KH(\tau)$. Since τ and m_1 commute,

$$e_1 = e_1^2 = \frac{1}{|A|}\tau m_1^2,$$

and

$$\frac{1}{|A|}\tau m_1 = \frac{1}{|A|}\tau m_1^2.$$

By the observation preceding the theorem, $m_1 = m_1^2$. Arguing in the same way, m_1, m_2 are orthogonal idempotents in $KH(\tau)$. Since

$$\frac{1}{|A|}\tau f = \frac{1}{|A|}\tau(m_1 + m_2),$$

the same observation implies $f = m_1 + m_2$, a contradiction, proving the theorem.

3.5.2 Proof of the M-W theorem

By Theorem 32, $\frac{1}{|A|}\tau f_r^\tau$, $\tau \in A^*$, $1 \le r \le r_\tau$, is a primitive idempotent in KG. Since τ and f_r^τ commute the collection of products (5) is a system of primitive orthogonal idempotents for KG. Since

$$\frac{1}{|A|}\sum_{\tau\in A^*}\sum_{r=1}^{r_\tau}\tau f_r^\tau = \frac{1}{|A|}\sum_{\tau\in A^*}\tau\left(\sum_{r=1}^{r_\tau} f_r^\tau\right) = \frac{1}{|A|}\sum_{\tau\in A^*}\tau = 1,$$

the system is complete, proving the theorem.

3.6 Abelian Extension

The M-W theorem will be used to construct an algorithm for computing complete system of primitive orthogonal idempotents for abelian extensions. We begin by assuming that Δ is a subgroup of a semidirect product $G = A \leftthreetimes B$ of finite abelian groups A and B. By the M-W algorithm, we can build a complete system of primitive orthogonal idempotents for G from the characters of A. The approach can be tailored to the subgroup Δ.

The projection $P : G \longrightarrow B$ defined by

$$Px = z, \quad x \in G, x = yz, y \in A, z \in B,$$

is a group homomorphism of G onto B having kernel A. Since $\Delta \subset A \not\triangleleft P\Delta$, where $P\Delta$ is a subgroup of B, we can assume without loss of generality that $B = P\Delta$.

Suppose ρ is a character of A. Define

$$\{B_1 = \{z \in B : [z, \Delta] \subset ker(\rho)\}$$

and

$$\Delta_1 = \{x \in \Delta : Px \in B_1\}.$$

B_1 is a subgroup of B and Δ_1 is a subgroup of Δ containing $\Delta \cap A$.

For $x_1 \in \Delta_1$, $x = yz$, $y \in A$ and $z \in B_1$, define

$$\rho_1(x) = \rho(y).$$

Theorem 33 *ρ_1 is a character of Δ_1 extending the restriction of ρ to $\Delta \cap A$.*

Proof Suppose $x_1, x_2 \in \Delta_1$ and write $x_1 = y_1z_1$, $x_2 = y_2z_2$, $y_1, y_2 \in A$, $z_1, z_2 \in B_1$. Since

$$x_1x_2 = [z_1, x_1]y_1y_2z_1z_2$$

and $[z_1, x_2] \in ker(\rho)$,

$$\rho_1(x_1x_2) = \rho_1(x_1)\rho_1(x_2),$$

proving ρ_1 is a character of Δ_1. Clearly, ρ_1 extends the restriction of ρ to $\Delta \cap A$.

The critical condition used in this theorem is that

$$\Delta_1 \subset A \not\triangleleft B_1,$$

with $[B_1, \Delta_1] \subset ker(\rho)$ which implies that ρ_1 is a character of Δ_1. In general ρ_1 is *not* a maximal extension in Δ of the restriction of ρ to $\Delta \cap A$. For this to occur we require that

$$\Delta_1 = \{x \in \Delta : [x, \Delta_1] \subset ker(\rho)\}.$$

Define

$$B_2 = \{z \in B : [z, \Delta_1] \subset ker(\rho)\}$$

and

$$\Delta_2 = \{x \in \Delta : Px \in B_2\}.$$

B_2 is a subgroup of B containing B_1 and Δ_2 is a subgroup of Δ containing Δ_1.

Theorem 34

$$\Delta_2 = \{x \in \Delta : [x, \Delta_1] \subset ker(\rho)\}.$$

Proof Suppose $x \in \Delta_2$ with $x = yz$, $y \in A$, $z \in B_2$. For any $x_1 \in \Delta_1$, with $x_1 = y_1 z_1$, $y_1 \in A$, $z_1 \in B_1$, we have

$$[x, z_1] \in ker(\rho), \quad [z, x_1] \in ker(\rho)$$

implying

$$[x, x_1] = [z, x_1][x, z_1] \in ker(\rho).$$

Since x_1 is arbitrary in Δ_1, $[x, \Delta_1] \in ker(\rho)$ and we have shown that

$$\Delta_2 \subset \{x \in \Delta : [x, \Delta_1] \subset ker(\rho)\}.$$

Conversely, take $x \in \Delta$ such that $[x, \Delta_1] \subset ker(\rho)$. For any $x_1 \in \Delta_1$, $[x, x_1] \in ker(\rho)$. Since $[x, z_1] \in ker(\rho)$, and

$$[x, x_1] = [z, x_1][x, z_1] \in ker(\rho),$$

we have $[z, x_1] \in ker(\rho)$ and $z \in B_2$. This shows that $x \in \Delta_2$, completing the proof.

If $\Delta_1 = \Delta_2$, then ρ_1 is a maximal extension in Δ of the restriction of ρ to $\Delta \cap A$ and $\frac{1}{|\Delta_1|}\rho_1$ is an idempotent in $\mathbf{C}\Delta$. Otherwise, define

$$B_3 = \{z \in B : [z, \Delta_2] \subset ker(\rho)\}$$

and

$$\Delta_3 = \{x \in \Delta : Px \in B_3\}.$$

Since

$$[B_1, \Delta_2] \subset [B_1, \Delta] \subset ker(\rho),$$

we have that B_1 is a subgroup of B_3. In the same way,

$$[B_3, \Delta_1] \subset [B_3, \Delta_2] \subset ker(\rho),$$

implies B_3 is a subgroup of B_2. We have shown

$$\Delta_1 \subset \Delta_3 \subset \Delta_2 \subset \Delta.$$

Replacing Δ by Δ_2 and Δ_1 by Δ_3 we can continue in this way and construct a subgroup B_M of B such that the subgroup Δ_M of Δ defined by

$$\Delta_M = \{x \in \Delta : Px \in B_M\}$$

satisfies the two conditions

$$[\Delta_M, B_M] \subset ker(\rho)$$
$$\Delta_M = \{x \in \Delta : [x, \Delta_M] \subset ker(\rho)\}.$$

The first implies that the mapping $\rho_M : \Delta_M \longrightarrow \mathbf{C}^\times$ defined by

$$\rho_M(x) = \rho(y), \quad x \in \Delta_M, x = yz, y \in A, z \in B_M$$

is a character of Δ_M extending the restriction of ρ to $\Delta \cap A$. The second shows that ρ_M is a maximal character extension in Δ of the restriction of ρ to $\Delta \cap A$ and $\frac{1}{|\Delta_M|}\rho_M$ is an idempotent in $\mathbf{C}\Delta$.

3.7 Equivalence

Many of the most important results on the structure of the algebra $\mathbf{C}G$ are described in terms of two-sided G-invariant subspaces of $\mathbf{C}G$. We will see that $\mathbf{C}G$ decomposes into the direct sum of all its irreducible two-sided G-invariant subspaces. This is the first step in proving the Wedderburn structure theorem which constructs a faithful representation of $\mathbf{C}G$ as the direct sum of complete matrix algebras over $\mathbf{C}$.

The decomposition of $\mathbf{C}G$ into the direct sum of its irreducible two-sided G-invariant subspaces is necessarily unique. The analogous statement for irreducible G-invariant subspaces does not hold, but will up to equivalence between such spaces. Equivalent irreducible G-invariant subspaces are the building blocks for the irreducible two-sided G-invariant subspaces.

These results extend the classical DSP algorithm for computing cyclic convolutions by fast Fourier transforms and diagonal matrix multiplications. For nonabelian groups, the diagonal matrix multiplications are replaced by block-diagonal matrix multiplications. This result is called the Wedderburn Structure theorem which has many generalizations.

For $\alpha \in \mathbf{C}G$, *right-translation* by α is the $\mathbf{C}$-linear transformation $R(\alpha)$ of $\mathbf{C}G$ defined by

$$R(\alpha)f = f\alpha, \quad f \in \mathbf{C}G.$$

By the associative law in $\mathbf{C}G$, $R(\alpha)$ commutes withe all *left*-translations of $\mathbf{C}G$,

$$R(\alpha)(\beta f) = \beta R(\alpha)f, \quad \beta, f \in \mathbf{C}G. \tag{6}$$

In fact any mapping T of $\mathbf{C}G$ into itself satisfying (6) is right-translation by $T(1)$,

$$T(f) = T(f \cdot 1) = fT(1), \quad f \in \mathbf{C}G.$$

Suppose W is a G-invariant subspace of $\mathbf{C}G$. For $\alpha \in \mathbf{C}G$, denote by $R_W(\alpha)$ the restriction of $R(\alpha)$ to W. $R_W(\alpha)$ is a $\mathbf{C}$-linear transformation of W onto $W\alpha$,

$$W\alpha = \{f\alpha : f \in W\}.$$

$W\alpha$ is a G-invariant subspace of $\mathbf{C}G$ by (6). It may be the $\{0\}$ subspace.

Suppose e is a generating idempotent for the G-invariant subspace W. A mapping T of W into $\mathbf{C}G$ satisfying

$$T(\beta f) = \beta T(f), \quad \beta, f \in W,$$

equals $R_W(\alpha)$ where $\alpha = T(e)$.

The following results of Schur describe right-translations on irreducible G-invariant subspaces and serve as important tools throughout this chapter.

Theorem 35 *If W is an irreducible G-invariant subspace and $\alpha \in \mathbf{C}G$, then $W\alpha = \{0\}$ or $W\alpha$ is an irreducible G-invariant subspace. If $W\alpha \neq \{0\}$, then $R_W(\alpha)$ is a $\mathbf{C}$-linear isomorphism of W onto $W\alpha$.*

Proof Suppose $W\alpha \neq \{0\}$ and $R_W(\alpha)$ is not a $\mathbf{C}$-linear isomorphism. Then

$$V = \{f \in W : f\alpha = 0\} \neq \{0\}$$

is a G-invariant subspace of W. By irreducibility, $V = W$ and $W\alpha = \{0\}$, a contradiction, proving $R_W(\alpha)$ is a $\mathbf{C}$-linear isomorphism of W onto $W\alpha$.

Suppose $W\alpha \neq \{0\}$ and U is a G-invariant subspace of $W\alpha$. Then

$$\{f \in W : f\alpha \in U\}$$

is a G-invariant subspace of W. It is either the $\{0\}$ subspace and $U = \{0\}$ or it is W and $U = W\alpha$, proving $W\alpha$ is irreducible and completing the proof.

Corollary 17 *If $W\alpha \neq \{0\}$ and e' is a generating idempotent for $W\alpha$, then there exists a unique $h \in W$ such that $e' = h\alpha$. We have*

- $R_{W\alpha}(h)R_W(\alpha) = I_W$,
- $R_W(\alpha)R_{W\alpha}(h) = I_{W\alpha}$,
- $(W\alpha)_h = W$.

Proof Since $R_W(\alpha)$ is a $\mathbf{C}$-linear isomorphism of W onto $W\alpha$, there exists a unique $h \in W$ satisfying $e' = h\alpha$. To complete the proof we need only to prove the second statement. Take $g \in W\alpha$. Then $ge' = g$ and

$$(gh)\alpha = g(h\alpha) = ge' = g,$$

completing the proof.

For an irreducible G-invariant subspace W of $\mathbf{C}G$ we can have $W = W\alpha$ for some $\alpha \in \mathbf{C}G$. For example, if e is a generating idempotent for W, then $W = We$ and $R_W(e) = I_W$. We have the following result of Schur.

Theorem 36 *Suppose W is an irreducible G-invariant subspace of $\mathbf{C}G$. If $\alpha \in \mathbf{C}G$ such that $W = W\alpha$, then there exists $a \in \mathbf{C}^\times$ such that*

$$R_W(\alpha) = aI_w.$$

Proof By Theorem 35, $R_W(\alpha)$ is a $\mathbf{C}$-linear automorphism of W. Since $\mathbf{C}$ is algebraically closed, $R_W(\alpha)$ has an eigenvalue $a \in \mathbf{C}^\times$ and there exists a nonzero $f_0 \in W$ such that

$$f_0\alpha = af_0.$$

Consider

$$W(a) = \{f \in W : R_W(\alpha)f = af\}.$$

For $\beta \in \mathbf{C}G$ and $f \in W(a)$, since

$$(\beta f)\alpha = \beta(f\alpha) = a(\beta f),$$

we have $\beta f \in W(a)$ and $W(a)$ is a G-invariant subspace of W. Since $W(a) \neq \{0\}$, $W(a) = W$, completing the proof.

Corollary 18 *If e is a generating idempotent for W, then for some $a \in \mathbf{C}^\times$,*

$$e\alpha = e\alpha e = ae.$$

Suppose W is an irreducible G-invariant subspace of $\mathbf{C}G$. A G-invariant subspace $W' \neq \{0\}$ is called *equivalent* to W if there exists $\alpha \in \mathbf{C}G$ such that $W' = W\alpha$. By Theorem 35 and its corollary, if W' is equivalent to W, then W' is irreducible and W is equivalent to W'. In this way we define an equivalence relation on the collection of irreducible G-invariant subspaces of $\mathbf{C}G$. Denote by W^R the collection of all irreducible G-invariant subspaces equivalent to W.

We have the following criterion for equivalence.

Theorem 37 *Suppose W and W' are irreducible G-invariant subspaces having generating idempotents e and e'. Then W and W' are equivalent if and only if there exits a* nonzero *$\gamma \in \mathbf{C}G$ satisfying*

$$\gamma = e\gamma = \gamma e' = e\gamma e'.$$

In this case $W' = W\gamma$.

Proof Suppose W and W' are equivalent and $W' = W\alpha$, $\alpha \in \mathbf{C}G$. Since $W = We$ and $W\alpha = (W\alpha)e'$, we have $W\alpha = We\alpha e'$. Setting $\gamma = e\alpha e'$,

$$\gamma = e\gamma = \gamma e' = e\gamma e' \neq 0,$$

and $W' = W\gamma$.

Conversely if there exists $\gamma \neq 0$ in $\mathbf{C}G$ satisfying

$$\gamma = e\gamma = \gamma e' = e\gamma e',$$

then $W\gamma \subset W'$. $W\gamma$ is a nonzero subspace of W' and $W' = W\gamma$, completing the proof.

We need assume in the theorem that $\gamma = e\gamma e' \neq 0$ since $\gamma = e\gamma e'$ implies $\gamma = e\gamma$ and $\gamma = \gamma e'$.

For the following discussion, we write $U \sim V$ to mean that the irreducible G-invariant subspaces U and V are equivalent. Consider a direct sum decomposition of a G-invariant subspace W of $\mathbf{C}G$,

$$W = \sum_{t=1}^{T} \oplus W_t,$$

into irreducible G-invariant subspaces W_t, $1 \leq t < T$. We will show that up to equivalence such decompositions are unique. The main result needed is the following.

Theorem 38 *If V is an irreducible G-invariant subspace contained in W, then*

$$V \subset \sum_{W_t \sim V} \oplus W_t,$$

the direct sum taken over all W_t equivalent to V, $1 \leq t \leq T$.

Proof Suppose e is a generating idempotent for V and write

$$e = \sum_{t=1}^{T} \alpha_t, \quad \alpha_t \in W_t.$$

We have that

$$V \subset \sum_{\alpha_t \neq 0} \oplus W_t.$$

Since e is an idempotent

$$e = e^2 = \sum_{t=1}^{T} e\alpha_t, \quad e\alpha_t \in W_t.$$

Uniqueness of representation in the direct sum implies

$$e\alpha_t = \alpha_t, \quad 1 \leq t \leq T.$$

For any $1 \leq t \leq T$ such that $\alpha_t \neq 0$, we have $e\alpha_t \neq 0$ and

$$\{0\} \neq V\alpha_t \subset W_t.$$

Irreducibility implies

$$V\alpha_t = W_t, \quad \alpha_t \neq 0$$

and $W_t \sim V$, completing the proof.

Corollary 19 *Suppose V_s, $1 \leq s \leq S$, is a set of equivalent irreducible G-invariant subspaces contained in W. Then $\sum_{s=1}^{S} V_s \subset \sum_{W_t \sim V_1} \oplus W_t$.*

Consider any set of irreducible G-invariant subspaces V_{s_1}, $1 \leq s_1 \leq S_1$ such that every V_s, $1 \leq s \leq S$, is equivalent to a unique V_{s_1}, $1 \leq s_1 \leq S_1$.

Corollary 20 *For $1 \leq s_1 \leq S_1$,*

$$\sum_{V_s \sim V_{s_1}} V_s \subset \sum_{W_t \sim V_{s_1}} \oplus W_t.$$

By the proceeding theorem and its corollaries, if W has two direct sum decompositions into irreducible G-invariant subspaces

$$W = \sum_{t=1}^{T} \oplus W_t = \sum_{s=1}^{S} \oplus V_s,$$

up to rearrangement of the factors, W_s is equivalent to V_s, $1 \leq s \leq S$ and by dimension $S \leq T$. Reversing the roles, we have the following result.

Theorem 39 *Suppose $W = \sum_{t=1}^{T} W_t = \sum_{s=1}^{S} \oplus V_s$ are direct sum decompositions of a G-invariant subspace W into irreducible G-invariant subspaces W_t, $1 \leq t < T$, and V_s, $1 \leq s \leq S$. Then $T = S$ and up to rearrangement, W_t is equivalent to V_t, $1 \leq t \leq T$.*

3.7.1 Two-Sided

A G-invariant subspace J of $\mathbf{C}G$ is called *two-sided* if J is invariant under all right-translations,

$$J\alpha \subset J, \quad \alpha \in \mathbf{C}G.$$

A nonzero two-sided G-invariant subspace J is called *irreducible* if the only two-sided G-invariant subspaces of J are $\{0\}$ and J. An arbitrary two-sided G-invariant subspace partitions the collection of all irreducible two-sided G-invariant subspaces into two sets; those contained in J and those having trivial intersection with J.

Suppose W is a G-invariant subspace and J and J' are two-sided G-invariant subspaces. WJ is a two-sided G-invariant subspace contained in J and JW is a G-invariant subspace contained in $J \cap W$. In particular JJ' is two-sided and is contained in $J \cap J'$. For a direct sum $J \oplus J'$ we have $JJ' = J'J \subset J \cap J' = \{0\}$.

Suppose W is an irreducible G-invariant subspace of $\mathbf{C}G$ and J is a two-sided G-invariant subspace. W^R denotes the collection of all irreducible G-invariant subspaces equivalent to W. For $\alpha \in J$, we have either $W\alpha = \{0\}$ or $W\alpha \in W^R$. Since $W\alpha \in J$,

$$WJ \subset \cup_{W' \in W^R}(J \cap W') \tag{7}$$

In particular if $J \cap W' = \{0\}$for all $W' \in W^R$, then $WJ = \{0\}$.

Theorem 40 *Suppose J is a two-sided G-invariant subspace and W is an irreducible G-invariant subspace such that $J \cap W \neq \{0\}$. Then*

$$W' \subset J, \text{ for all } W' \in W^R.$$

Proof Since $J \cap W$ is a G-invariant subspace of W and $J \cap W \neq \{0\}$, we have $J \cap W = W$ and $W \subset J$. The invariance of J under right-translations implies $W\alpha \subset J$, for all $\alpha \in \mathbf{C}G$, completing the proof.

From the theorem a two-sided G-invariant subspace J partitions the set of all equivalence classes of irreducible G-invariant subspaces into two subsets, those having all its elements contained in J and those having all its elements having trivial intersection $\{0\}$ with J.

For an irreducible G-invariant subspace W of $\mathbf{C}G$, define

$$J(W) = \sum_{W' \in W^R} W'.$$

$J(W)$ is G-invariant and is the minimal G-invariant subspace containing all $W' \in W^R$.

Theorem 41 *$J(W)$ is an irreducible two-sided G-invariant subspace.*

For $\alpha \in \mathbf{C}G$ and $W' \in W^R$, we have $W'\alpha = \{0\}$ or $W'\alpha \in W^R$. From

$$J(W)\alpha = \sum_{W' \in W^R} W'\alpha \subset \sum_{W' \in W^R} W' = J(W), \quad \alpha \in \mathbf{C}G,$$

$J(W)$ is a two-sided G-invariant subspace.

Suppose $J \neq \{0\}$ is a two-sided G-invariant subspace contained in $J(W)$. If e is a generating idempotent for $J(W)$,

$$J = Je \subset JJ(W) \neq \{0\}.$$

Assume $J \cap W' = \{0\}$, for all $W' \in W^R$. Then

$$JW' \subset J \cap W' = \{0\}, \text{ for all } W' \in W^R,$$

and $JJ(W) = \{0\}$, a contradiction. We must have

$$J \cap W' \neq \{0\}, \text{ for some } W' \in W^R,$$

which by Theorem 40 implies $J = J(W)$. $J(W)$ is irreducible, completing the proof.

By Theorem 39, $J(W)$ has an essentially unique direct sum decomposition into irreducible G-invariant subspaces

$$J(W) = \sum_{s=1}^{S} \oplus V_s. \tag{8}$$

Choose $T \leq S$ such that, perhaps up to reordering of the factors in (8), every V_s, $1 \leq s \leq S$, is equivalent to exactly *one* V_t, $1 \leq t \leq T$. We will show $T = 1$. Denote by J_t the direct sum of all the factors of (8) equivalent to V_t, $1 \leq t \leq T$. Then

$$J(W) = \sum_{t=1}^{T} \oplus J_t.$$

We will show that J_1 is a two-sided G-invariant subspace which by irreducibility of $J(W)$ implies $J_1 = J(W)$ and $T = 1$.

Theorem 42 *$J(W)$ is the direct sum of irreducible G-invariant subspaces all of which are equivalent to W.*

Proof Suppose V is any factor in the given direct sum decomposition of J_1. Since $J(W)\alpha \subset J(W)$, for all $\alpha \in \mathbf{C}G$,

$$V\alpha \subset \sum_{t=1}^{T} \oplus J_t, \text{ for all } \alpha \in \mathbf{C}G.$$

By Theorem 38, $V\alpha = \{0\}$ or $V\alpha$ is equivalent to V_1, implying

$$V\alpha \subset J_1, \text{ for all } \alpha \in \mathbf{C}G.$$

Since V is an arbitrary factor of the direct sum decomposition of J_1,

$$J_1\alpha \subset J_1, \text{ for all } \alpha \in \mathbf{C}G,$$

and J_1 is a two-sided G-invariant subspace, completing the proof.

Corollary 21 *Every irreducible G-invariant subspace of $J(W)$ is equivalent to W.*

Corollary 22 *Suppose*

$$\{W_s : 1 \leq s \leq S\}$$

is a set of pairwise inequivalent *irreducible G-invariant subspaces. Then the sum $\sum_{s=1}^{S} J(W_s)$ is a direct sum*

Proof By the preceding theorem, for $s \neq t$,

$$J(W_s)J(W_t) \subset J(W_s) \cap J(W_t) = \{0\}.$$

If

$$\sum_{t=1}^{S} \alpha_t = 0, \quad \alpha_t \subset J(W_t),$$

and e_s is an idempotent generator for $J(W_s)$, $1 \leq s \leq S$, then

$$\left(\sum_{t=1}^{S} \alpha_t\right) e_s = \alpha_s e_s = \alpha s = 0,$$

completing the proof.

Suppose J is a two-sided G-invariant subspace and $\Sigma(J)$ denotes the collection of all irreducible two-sided G-invariant subspaces contained in J. By Theorem 40, there exists a set

$$\{W_t : 1 \leq t \leq T\}$$

of irreducible G-invariant subspaces contained in J such that every irreducible G-invariant subspace contained in J is equivalent to exactly one W_t, $1 \leq t \leq T$, and $J(W_t) \subset J$, $1 \leq t \leq T$.

Theorem 43 $J = \sum_{t=1}^{T} \oplus J(W_t)$ *where*

$$\Sigma(J) = \{J(W_t) : 1 \leq t \leq T\}.$$

Proof By Corollary 18 of Theorem 42,

$$J = \sum_{t=1}^{T} \oplus J(W_t).$$

Suppose J' is an irreducible two-sided G-invariant subspace contained in J. If $J \cap J(W_t) = \{0\}$, for all $1 \leq t \leq T$, then $JJ' = \{0\}$, a contradiction. We must have

$$J' \cap J(W_t) \neq \{0\}, \text{ for some } 1 \leq t \leq T.$$

Irreducibility implies $J' = J(W_t)$, completing the proof.

Corollary 23 *J is the direct sum of all the irreducible two-sided G-invariant subspaces contained in J.*

Applying Theorem 43 and its corollary to $\mathbf{C}G$ we have the following result which we state as a theorem because of its importance.

Theorem 44 *$\mathbf{C}G$ is the direct sum of all its irreducible two-sided G-invariant subspaces.*

Corollary 24 *If J is a two-sided G-invariant subspace of $\mathbf{C}G$, then J', the direct sum of all the irreducible two-sided G-invariant subspaces having trivial intersection $\{0\}$ with J, is the unique two-sided G-invariant subspace of $\mathbf{C}G$ satisfying $\mathbf{C}G = J \oplus J'$.*

Corollary 25 *A two-sided G-invariant subspace $J \neq \{0\}$ has a unique idempotent generator e and e is central in $\mathbf{C}G$.*

Proof By the preceding corollary, $\mathbf{C}G = J \oplus J'$. Write

$$1 = e + e', \quad e \in J,\ e' \in J'.$$

e and e' are orthogonal idempotents generating J and J' as G-invariant subspaces. For $g \in \mathbf{C}G$,

$$g = g \cdot 1 = ge + ge' = 1 \cdot g = eg + e'g.$$

Since J and J' are two-sided, ge, $eg \in J$ and ge', $e'g \in J'$. Uniqueness of representation implies $eg = ge$ and e is central in $\mathbf{C}G$.

Suppose e_1 is also an idempotent generator of J. Since e is central,

$$e = ee_1 = e_1 e = e_1,$$

completing the proof.

Suppose J is a two-sided G-invariant subspace having a direct sum decomposition

$$J = \sum_{s=1}^{S} \oplus V_s,$$

into irreducible G-invariant subspaces V_s, $1 \leq s \leq S$. As in the discussion leading up to Theorem 42, after rearrangement if necessary, there exists $T \leq S$, such that every V_s, $1 \leq s \leq S$, is equivalent to exactly one V_t, $1 \leq t \leq T$, and

$$J = \sum_{t=1}^{T} \oplus J(V_t).$$

Denoting by J_t the direct sum of all the factors V_s, $1 \leq s \leq S$, equivalent to V_t, we have

$$J = \sum_{t=1}^{T} \oplus J_t.$$

In particular J_t is an irreducible two-sided G-invariant subspace.

4 Development of Fast Algorithms

4.1 Character extension

4.1.1 Construction of Primitive Idempotents

Assume that H is a normal subgroup of G and $H\backslash G$ is an abelian group splitting over the field K. Suppose ρ is a character of H over K. By Theorem 16 and the corollary to Theorem 25, if $H = G(\rho)$ then ρ cannot be extended and $\frac{1}{|H|}\rho$ is a primitive idempotent in KG. Suppose H is strictly contained in $G(\rho)$. The following algorithm constructs a nontrivial extension of ρ.
H is strictly contained in $G(\rho)$.

- Choose $y \in G(\rho)$ and $y \notin H$ and form H_1 the subgroup generated by H and y.
- Find the smallest positive integer R such that $y^R \in H$.
- Compute $\lambda = \rho(y^R)$.
- Find any R-th root α of λ in K, $\alpha^R = \lambda$, possible since $H\backslash G$ splits over K.
- Write every $x \in H_1$ uniquely in the form

$$x = uy^r, \quad u \in H,\ 0 \leq r < R.$$

- Construct the mapping $\rho_1 : H_1 \longrightarrow K^\times$ by

$$\rho_1(uy^r) = \rho(u)\alpha^r, \quad 0 \leq r < R.$$

ρ_1 is an extension of ρ to H_1.

By repeated use of the algorithm, possible since every subgroup of G containing H is normal in G, we can construct a subgroup M of $G(\rho)$ admitting an extension γ of ρ to M such that $M = G(\gamma)$. In this case $\frac{1}{|M|}\gamma$ can be extended no further and is a primitive idempotent in KG.

Theorem 28 can then be used construct the collection $\rho(M)$ of all extensions of ρ to M.

- For each $\tilde{\chi} \in (H\backslash M)^*$, form the mapping $\gamma^\chi : M \longrightarrow K^\times$, by

$$\gamma^\chi(x) = \tilde{\chi}(Hx)\gamma(x), \quad x \in M.$$

The collection $\rho(M)$ of all extensions of ρ to M is given by

$$\rho(M) = \{\gamma^\chi : \tilde{\chi} \in (H\backslash M)^*\}.$$

By Theorem 23 and the corollary to Theorem **??**, the collection

$$\left\{\frac{1}{|M|}\gamma : \gamma \in \rho(M)\right\}$$

is a system of primitive, pairwise orthogonal idempotents in KG satisfying, by Theorem 29,

$$\frac{1}{|H|}\rho = \frac{1}{|M|}\sum_{\gamma\in\rho(M)}\gamma.$$

For each character ρ of H over K, denote by M_ρ any subgroup of $G(\rho)$ which admits an extension γ of ρ satisfying $M_\rho = G(\gamma)$. Denote by $\rho(M_\rho)$ the collection of all extensions of ρ to M_ρ. Then

$$I(\rho) = \{\frac{1}{|M_\rho|}\gamma : \gamma \in \rho(M_\rho)\}$$

is a system of primitive, pairwise orthogonal idempotents for KG satisfying

$$\frac{1}{|H|}\rho = \sum_{f\in I(\rho)} f.$$

By Theorem 30,

$$I = \cup_{\rho\in H^*} I(\rho)$$

is a system of primitive, pairwise orthogonal idempotents for KG satisfying

$$\frac{1}{|H|}\sum_{\rho\in H^*}\rho = \sum_{f\in I} f.$$

For H an abelian group,

$$1 = \frac{1}{|H|}\sum_{\rho\in H^*}\rho$$

and the above construction leads to a complete system of primitive, pairwise orthogonal idempotents for KG.

Up to scalar multiple, the primitive idempotents of KG resulting from the algorithm are characters of subgroups of G. If H is abelian, then a complete system of primitive, pairwise orthogonal idempotents of KG can, up to constant multiple, be given by characters of subgroups of G. If H is not abelian this need no longer be the case.

4.1.2 Coefficient computation

For $y \in B$, define $\alpha_y \in \mathbf{C}A$ by

$$\alpha_y(x) = \alpha(xy), \quad x \in A,$$

and compute the Fourier transform of α_y over A,

$$\hat{\alpha_y}(\tau) = \frac{1}{L}\sum_{x\in A}\alpha_y(x)\tau(x^{-1}), \quad \tau \in A^*.$$

M Fourier transforms over A are required at this stage. Place the results into a two-dimensional array over $A^* \times B$

$$\hat{\alpha}(\tau, y) = \hat{\alpha_y}(\tau), \quad \tau \in A^*,\ y \in B.$$

For each $\tau \in A^*$ we will compute the coefficients

$$\alpha_{\tau\lambda}(s), \quad 1 \le s \le S_\tau,\ \lambda \in B(\tau)^*.$$

For $1 \le s \le S_\tau$, define $\gamma_s^\tau \in \mathbf{C}B(\tau)$ by

$$\gamma_s^\tau(z) = \hat{\gamma}(\tau^{y_s}, y_s z), \quad z \in B(\tau),\ y_s = y_s^\tau,$$

and compute the Fourier transform of γ_s^τ over $B(\tau)$

$$\hat{\gamma_s^\tau}(\lambda) = \frac{1}{M_\tau} \sum_{z \in B(\tau)} \gamma_s^\tau(z)\lambda(z^{-1}), \quad \lambda \in B(\tau)^*.$$

S_τ Fourier transforms over $B(\tau)$ are required in this stage. Implementing this stage as τ runs over A^* requires $\sum_{\tau \in A^*} S_\tau$ Fourier transforms over abelian groups over varying sizes.

By theorem 17, for each $\tau \in A^*$,

$$\alpha_{\tau\lambda}(s) = \hat{\gamma_s^\tau}(\lambda), \quad \lambda \in B(\tau)^*,\ 1 \le s \le S_\tau.$$

First Stage $\alpha \in \mathbf{C}G$

$\downarrow$

$\alpha_y \in \mathbf{C}A,\ y \in B$

$\downarrow$ FT **over** $A,\ y \in B$.

$\hat{\alpha}_t \in \mathbf{C}A^*,\ y \in B$

$\downarrow$

$\hat{\alpha} \in L(A^* \times B)$

Second Stage $\tau \in A^*$

$\hat{\alpha} \in L(A^* \times B)$

$\downarrow$

$\gamma_s^\tau \in \mathbf{C}B(\tau),\ 1 \le s \le S_\tau$

$\downarrow$ FT over $B(\tau),\ 1 \le s \le S_\tau$.

$\hat{\gamma_s^\tau} \in \mathbf{C}B(\tau)^*,\ 1 \le s \le S_\tau$

$$\alpha_{\tau\lambda}(s) = \hat{\gamma_s^\tau}(\lambda), \quad \lambda B(\tau)^*,\ 1 \le s \le S_\tau.$$

4.2 Algorithm $G = A \leftthreetimes (B \leftthreetimes C)$

For $\tau \in A^*$

- Compute by the primitive idempotent construction algorithm a complete system of primitive, pairwise orthogonal idempotents for $KH(\tau)$,

$$f_\tau^r, \quad 1 \leq r \leq r_\tau.$$

- Form the products

$$\tau f_\tau^r, \quad 1 \leq r \leq r_\tau.$$

The collection of products

$$\frac{1}{|A|}\tau f_\tau^r, \quad \tau \in A^*, \, 1 \leq r \leq r_\tau,$$

is a complete system of primitive, pairwise orthogonal idempotents for KG.

Up to a constant multiple, the idempotents of $KH(\tau)$, $\tau \in A^*$, constructed in the algorithm are characters of $H(\tau)$. As a result, up to a constant multiple, the system of idempotents of KG resulting from the algorithm consists of characters of subgroups of G containing A. This is the case, even though $A\backslash G$ is not abelian.

By the Mackey-Wigner (M-W) little group theorem, we can accomplish the first task by designing an algorithm which, for each $\tau \in A^*$, computes a complete primitive idempotent system in $KH(\tau)$. In the next section, we develop an algorithm for this purpose based on the algorithms for $A \leftthreetimes B$. As we will see, combined with the M-W algorithm, this leads to primitive idempotents of KG which are characters of subgroups of $A \leftthreetimes H(\tau)$. We make critical use of this property in the design of the basis and expansion coefficient algorithms established in section 4.

4.2.1 Idempotent Systems for Subgroups of $H = B \leftthreetimes C$

Suppose Δ is a subgroup of H. Since B and C are abelian groups, $\Delta \cap B$ is an abelian, normal subgroup of Δ and $\Delta/\Delta \cap B$ is an abelian group. The algorithms for previous efforts apply.

Algorithm I Complete primitive idempotent system in $K\Delta$

A

For $\rho \in (\Delta \cap B)^*$

- Construct a subgroup Δ_ρ of Δ admitting an extention γ of ρ such that $\frac{1}{|\Delta_\rho|}\gamma$ is a primitive idempotent in $K\Delta$.
- Construct $\mathrm{ext}_\rho \Delta_\rho$, the collection of all extensions of ρ to Δ_ρ.
- Form the set

$$Idem(\rho) = \{\frac{1}{|\Delta_\rho|}\delta : \delta \in \mathrm{ext}_\rho \Delta_\rho\}.$$

$Idem(\rho)$ is an idempotent system in $K\Delta$ satisfying

$$\frac{1}{|B \cap \Delta|}\rho = \frac{1}{|\Delta_\rho|} \sum_{e \in Idem(\rho)} e.$$

B

- Implement A for all $\rho \in (B \cap \Delta)^*$.
- Form the set

$$\cup_{\rho \in (B \cap \Delta)^*} Idem(\rho).$$

Since $\Delta \cap B$ is an abelian group splitting over K, the collection

$$\cup_{\rho \in (B \cap \Delta)^*} Idem(\rho)$$

is a complete primitive idempotent system in $K\Delta$.

Combining this algorithm with the M-W algorithm, we have the following algorithm for constructing an idempotent system for KG.

Algorithm II Complete primitive idempotent system in KG

A

For $\tau \in A^*$,

- Apply algorithm I to construct a complete primitive idempotent system in $KH(\tau)$.

$$f_r^\tau, \quad 1 \leq r \leq r_\tau.$$

- Compute the products

$$\tau f_r^\tau, \quad 1 \leq r \leq r_\tau.$$

B

- Implement A for all $\tau \in A^*$.
- Form the set

$$\{\tau f_r^\tau : \tau \in A^*, 1 \leq r \leq r_\tau\}.$$

By the M-W algorithm this set is a complete primitive idempotent system in KG.

To establish notation for the following sections, we will explicitly describe A in algorithm II.

Algorithm III Step A of algorithm II

A'

For $\rho \in (H(\tau) \cap B)^*$,

- Construct a subgroup $H(\tau)_\rho$ of $H(\tau)$ admitting an extension γ of ρ such that $\frac{1}{|H(\tau)_\rho|}\gamma$ is a primitive idempotent in $KH(\tau)$.

- Construct the collection $\text{ext}_\rho H(\tau)_\rho$ of all extensions of ρ to $H(\tau)_\rho$.
- Form the set

$$Idem_\tau(\rho) = \{\frac{1}{|H(\tau)_\rho|}\delta : \delta \in \text{ext}_\rho H(\tau)_\rho\}.$$

B'

- Implement A' for all $\rho \in (H(\tau) \cap B)^*$.
- Form

$$Idem(\tau) = \cup_{\rho \in (H(\tau)\cap B)^*} Idem_\tau(\rho).$$

$Idem(\tau)$ is a complete primitive idempotent system in $KH(\tau)$.

4.2.2 Basis Algorithm

The primitive idempotents in KG resulting from algorithm II are constant multiples of characters of subgroups of G. The basis algorithm developed in this section and the expansion coefficient algorithm of the next section significantly depend on this form of the primitive idempotents.

Suppose $\tau \in A^*$, $\rho \in (B \cap H(\tau))^*$ and $H(\tau)_\rho$ and $\text{ext}_\rho H(\tau)_\rho$ are constructed by algorithm III. We will design an algorithm for constructing a basis for the irreducible G-invariant subspaces $KG\tau\gamma$, $\gamma \in \text{ext}_\rho H(\tau)_\rho$.

Choose a complete system of representatives

$$u_l, \quad 1 \le l \le L,$$

for the space of right $H(\tau)_\rho$-cosets in H. Every $y \in H$ has a unique representation of the form

$$y = u_l w, \quad 1 \le l \le L, w \in H(\tau)_\rho.$$

In general, u_l, $1 \le l \le L$, and L depend on τ and ρ but for the most part we suppress this dependence in the following discussion.

For $t \in G$, we can uniquely write

$$t = xy = xu_l w, \quad x \in A, y \in H, 1 \le l \le L, w \in H(\tau)_\rho.$$

$$\begin{aligned} t\tau\gamma &= xu_l w\tau\gamma = xu_l\tau u_l^{-1}u_l\tau w\gamma \\ &= \tau_l(x^{-1})\gamma(w^{-1})u_l\tau\gamma, \end{aligned}$$

where $\tau_l = u_l\tau u_l^{-1}$, $1 \le l \le L$. Since the set $\{t\tau\gamma : t \in G\}$ spans $KG\tau\gamma$, the set $\{u_l\tau\gamma : 1 \le l \le L\}$ spans $KG\tau\gamma$.

Theorem 45 *Suppose $\tau \in A^*$, $\rho \in (B \cap H(\tau))^*$ and u_l, $1 \le l \le L$, is a complete system of representatives for the $H(\tau)_\rho$-cosets in H. Then*

$$\{u_l\tau\gamma : 1 \le l \le L\}$$

is a basis of $KG\tau\gamma$, for every $\gamma \in \text{ext}_\rho H(\tau)_\rho$.

Proof We must prove linear independence. Suppose

$$\sum_{l=1}^{L} \alpha(l) u_l \tau \gamma = 0, \quad \alpha(l) \in K.$$

For $1 \leq m \leq L$,

$$\tau_m \sum_{l=1}^{L} \alpha(l) \tau_l u_l \gamma = 0,$$

where $\tau_l = u_l \tau u_l^{-1}$, $1 \leq l \leq L$. Since $\tau_m \tau_l = 0$ unless $\tau_m = \tau_l$, in which case $\tau_m^2 = |A| \tau_m$, we have

$$\sum_{u_m^{-1} u_l \in H(\tau)} \alpha(l) u_l \tau \gamma = 0,$$

where the sum is over all $1 \leq l \leq L$ such that $u_m^{-1} u_l \in H(\tau)$. We have used the equivalence between $\tau_m = \tau_l$ and $u_m^{-1} u_l \tau u_l^{-1} u_m = \tau$. Multiplying by u_m^{-1},

$$u_m^{-1} \sum_{u_m^{-1} u_l \in H(\tau)} \alpha(l) u_l \tau \gamma = \sum_{u_m^{-1} u_l \in H(\tau)} \alpha(l) \tau u_m^{-1} u_l \gamma = 0.$$

Since $H(\tau)_\rho$ is a normal subgroup of $H(\tau)$ and is the centralizer of γ in $H(\tau)$, we have, arguing as above, that

$$\sum_{u_m^{-1} u_l \in H(\tau)_\rho} \alpha(l) u_l \tau \gamma = 0.$$

This sum has only one term implying

$$\alpha(m) u_m \tau \gamma = 0$$

and $\alpha(m) = 0$. Since $1 \leq m \leq L$ is arbitrary, $\alpha(m) = 0$, $1 \leq m \leq L$, completing the proof.

In the following algorithm, we suppress the construction of centralizer subgroups.

Algorithm IV Basis for $KG\tau\lambda$
For $\tau \in A^*$ and $\rho \in (B \cap H(\tau))^*$,

- Construct $H(\tau)_\rho$ and $\mathrm{ext}_\rho H(\tau)_\rho$ by algorithm III.
- Construct u_l, $1 \leq l \leq L$, a complete system of right $H(\tau)_\rho$-cosets in H.

For $\gamma \in \mathrm{ext}_\rho H(\tau)_\rho$,

- Compute the products

$$u_l \tau \gamma, \quad 1 \leq l \leq L.$$

By the theorem, $\{u_l \tau \gamma : 1 \leq l \leq L\}$ is a basis of $KG\tau\gamma$.

4.2.3 Expansion Coefficient Algorithm

Suppose $\tau \in A^*$, $\rho \in (B \cap H(\tau))^*$, $H(\tau)_\rho$ and $\mathrm{ext}_\rho H(\tau)_\rho$ are constructed by algorithm III, and u_l, $1 \le l \le L$, is a complete system of right $H(\tau)_\rho$-coset representatives in H.

Consider $\alpha \in KG$. The component of α in the irreducible G-invariant subspace $KG\tau\gamma$ is

$$\frac{1}{|G(\tau)_\rho|}\alpha\tau\gamma, \quad \gamma \in \mathrm{ext}_\rho H(\tau)_\rho,$$

where $G(\tau)_\rho = A \leftthreetimes H(\tau)_\rho$. Relative to the basis

$$u_l\tau\gamma, \quad 1 \le l \le L,$$

of $KG\tau\gamma$, we can write

$$\alpha\tau\gamma = \sum_{l=1}^{L} \alpha_{\tau\gamma}(l)u_l\tau\gamma, \quad \alpha_{\tau\gamma}(l) \in K, \gamma \in \mathrm{ext}_\rho H(\tau)_\rho.$$

Theorem 46 *For $\gamma \in \mathrm{ext}_\rho H(\tau)_\rho$,*

$$\alpha_{\tau\gamma}(l) = \sum_{w \in H(\tau)_\rho} \left(\sum_{x \in A} \alpha(xu_lw)\tau_l(x^{-1}) \right) \gamma(w^{-1}), \quad 1 \le l \le L,$$

where $\tau_l = u_l\tau u_l^{-1}$, $1 \le l \le L$.

Proof By the results in 46, for every $t \in G$, we can uniquely write

$$t = xu_lw, \quad x \in A, 1 \le l \le L, w \in H(\tau)_\rho,$$

and we have

$$t\tau\gamma = \tau_l(x^{-1})\gamma(w^{-1})u_l\tau\gamma.$$

Then

$$\alpha\tau\gamma = \sum_{t \in G} \alpha(t)t\tau\gamma = \sum_{l=1}^{L} \left(\sum_{w \in H(\tau)_\rho} \left(\sum_{x \in A} \alpha(xu_lw)\tau_l(x^{-1}) \right) \gamma(w^{-1}) \right) u_l\tau\gamma,$$

completing the proof.

Algorithm V Expansion coefficients

Suppose $\alpha = \sum_{t \in G} \alpha(t)t = \sum_{y \in H} \sum_{x \in A} \alpha(xy)xy$ is in KG.

A. For $y \in H$,

- Form $\alpha_y : A \longrightarrow K$ by
$$\alpha_y(x) = \alpha(xy), \quad x \in A.$$
- Compute $\hat{\alpha}_y : A^* \longrightarrow K$ by
$$\hat{\alpha}_y(\tau) = \sum_{x \in A} \alpha_y(x)\tau(x^{-1}), \quad \tau \in A^*.$$

linking

- Implement step A for every $y \in H$.
- Form $\chi : Y \times A^* \longrightarrow K$ by

$$\chi(y, \tau) = \hat{\alpha}_y(\tau), \quad y \in H, \tau \in A^*.$$

B. For $\tau \in A^*$ and $\rho \in (B \cap H(\tau))^*$,

- Construct $H(\tau)_\rho$ and $\mathrm{ext}_\rho H(\tau)_\rho$ (algorithm 9.3),
- Construct u_l, $1 \leq l \leq L$, a complete system of right $H(\tau)_\rho$-coset representatives in H,
- Form $\chi_l : H(\tau)_\rho \longrightarrow K$, $1 \leq l \leq L$, by

$$\chi_l(w) = \chi(u_l \tau u_l^{-1}, u_l w), \quad w \in H(\tau)_\rho,$$

- Compute $\widehat{\chi}_l : \mathrm{ext}_\rho H(\tau)_\rho \longrightarrow K$, $1 \leq l \leq L$, by

$$\widehat{\chi}_l(\gamma) = \sum_{w \in H(\tau)_\rho} \chi_l(w)\gamma(w^{-1}), \quad \gamma \in \mathrm{ext}_\rho H(\tau)_\rho.$$

By Theorem 46

$$\alpha_{\tau\gamma}(l) = \widehat{\chi}_l(\gamma), \quad \gamma \in \mathrm{ext}_\rho H(\tau)_\rho, \, 1 \leq l \leq L.$$

C. Implement stage B for all $\tau \in A^*$ and $\rho \in (B \cap H(\tau))^*$.

Stage C completes the computation of the expansion coefficient of α.

The stage B computations of $\widehat{\chi}_l$, $1 \leq l \leq L$, closely resemble Fourier transform computations but $H(\tau)_\rho$ is not necessarily abelian and the computations are taken only over $\gamma \in \mathrm{ext}_\rho H(\tau)_\rho$. We will show how to turn the main part of these computations into Fourier transform computations.

Choose a complete system v_j, $1 \leq j \leq J$, of right $(B \cap H(\tau))$-coset representatives in $H(\tau)_\rho$. Each $w \in H(\tau)_\rho$ can be uniquely written as

$$w = v_j u, \quad 1 \leq j \leq J, \, u \in B \cap H(\tau).$$

The computation of $\widehat{\chi}_l$, $1 \leq l \leq L$, can be written as

$$\begin{aligned} \widehat{\chi}_l(\gamma) &= \sum_{w \in H(\tau)_\rho} \chi_l(w)\gamma(w^{-1}) \\ &= \sum_{j=1}^{J} \gamma(v_j^{-1}) \sum_{u \in B \cap H(\tau)} \chi(u_l \tau u_l^{-1}, u_l v_j u)\rho(u^{-1}). \end{aligned} \tag{9}$$

Using this result we can replace step B by the following.

B'. For $\tau \in A^*$,

- Construct w_k, $1 \le k \le K$, a complete system of right $B \cap H(\tau)$-coset representatives in H,
- Form $\psi_k : B \cap H(\tau) \longrightarrow K$, $1 \le k \le K$, by

$$\psi_k(u) = \chi(w_k \tau w_k^{-1}, w_k u), \quad u \in B \cap H(\tau),$$

- Compute $\widehat{\psi}_k : (B \cap H(\tau))^* \longrightarrow K$, $1 \le k \le K$, by

$$\widehat{\psi}_k(\rho) = \sum_{u \in B \cap H(\tau)} \psi_k(u)\rho(u^{-1}), \quad \rho \in (B \cap H(\tau))^*.$$

C'. For $\rho \in (B \cap H(\tau))^*$,

- Construct u_l, $1 \le l \le L$, a complete system of right $H(\tau)_\rho$-coset representatives in H,
- Construct v_j, $1 \le j \le J$, a complete system of right $B \cap H(\tau)$-coset representatives in $H(\tau)_\rho$.

linking For each pair (l, j), $1 \le l \le L$, $1 \le j \le J$, there exists a unique $k(l, j)$, $1 \le k(l, j) \le K$ such that

$$u_l v_j = w_{k(l,j)} z_{(l,j)}, \quad z_{(l,j)} \in B \cap H(\tau).$$

- Compute the products

$$\widehat{\psi}_{l,j}(\rho) = \rho(z(l, j))\widehat{\psi}_{k(l,j)}(\rho), \quad 1 \le l \le L, 1 \le j \le J.$$

D'. For $\gamma \in \mathrm{ext}_\rho H(\tau)_\rho$,

- Compute the matrix product

$$\left[\widehat{\psi}_{l,j}(\rho)\right]_{1 \le l \le L, 1 \le j \le J} \begin{bmatrix} \gamma(v_1^{-1}) \\ \vdots \\ \gamma(v_J^{-1}) \end{bmatrix}.$$

By (9) the resulting vector is

$$\begin{bmatrix} \alpha_{\tau\gamma}(1) \\ \vdots \\ \alpha_{\tau\gamma}(L) \end{bmatrix}.$$

5 Code Development

Distinct realizations of an abstract group leads to a distinct unitary transformations, and distinct geometric identification properties.

Based on the algorithms of section 4, efficient codes implementing unitary transforms associated with several realizations of the following abstract groups have been developed.

- $(C_N \times C_N) \leftthreetimes C_2$,
- $(C_N \times C_N) \leftthreetimes (C_2 \times C_2)$,
- $(C_N \times C_N) \leftthreetimes (C_2 \times C_2 \times C_2)$,
- $(C_N \times C_N) \leftthreetimes (C_2 \times C_2 \times C_2 \times C_2)$,
- $(C_N \times C_N) \leftthreetimes C_3$,
- $(C_N \times C_N) \leftthreetimes C_4$,
- $(C_N \times C_N) \leftthreetimes C_6$,
- $(C_N \times C_N) \leftthreetimes ((C_2 \times C_2) \leftthreetimes C_2)$,
- $(C_N \times C_N) \leftthreetimes (C_4 \leftthreetimes C_2)$.
- $(C_N \leftthreetimes C_2) \times (C_M \leftthreetimes C_2)$,

These codes lead to efficient implementation of the nonabelian convolutions.

Fixing on a particular representation of $C_N \times C_N$, varying realizations of $G = (C_N \times C_N) \leftthreetimes H$ is achieved by constructing 2×2 integer matrices of finite order, modulo N. For example, a realization of the group $(C_N \times C_N) \leftthreetimes (C_2 \times C_2)$ is achieved by constructing 2×2 integer matrices of order 2 modulo N, that commute. Viewing the elements of $C_N \times C_N$ as column vectors of length 2, the group multiplication in G is identified with matrix multiplication.

Geometric properties of such realizations depend on the following.

- The integer N.
- The integer matrices of finite order, modulo N.
- Interaction between the integer matrices.

5.1 Examples

Denote the elements of $C_N \times C_N$ by $a^m b^n$, $0 \leq m, n \leq N-1$, and characters of $C_N \times C_N$ by $\alpha_k \beta_l$, $0 \leq k, l \leq N-1$,

$$\alpha_k \beta_l = \sum_{n=0}^{N-1} \sum_{m=0}^{N-1} exp(2\pi i \frac{km+ln}{N}) a^m b^n.$$

Denoting the generators of $C_2 \times C_2$ by s and t, complete system of orthogonal idempotents of $C_2 \times C_2$ are

$$\frac{1}{4}(1+s+t+st),\ \frac{1}{4}(1-s+t-st),\ \frac{1}{4}(1+s-t-st),\ \frac{1}{4}(1-s-t+st).$$

Primitive idempotents of $\mathbf{C}\left((C_N \times C_N) \leftthreetimes (C_2 \times C_2)\right)$ are of dimensions 1, 2 or 4. The number, dimension and characteristics of primitive idempotents depend on specific realizations of $C_2 \times C_2$.

Each realization is identified by a group of 4 commuting integer matrices of order 2. Any 2×2 commuting matrices σ and τ determines a realization of $(C_N \times C_N) \leftthreetimes (C_2 \times C_2)$ as follows. Set

$$s \leftrightarrow \sigma = \begin{bmatrix} s_1 & s_2 \\ s_3 & s_4 \end{bmatrix},$$

$$t \leftrightarrow \tau = \begin{bmatrix} t_1 & t_2 \\ t_3 & t_4 \end{bmatrix},$$

and for $0 \leq m, n < N$, let

$$\begin{bmatrix} m_s \\ n_s \end{bmatrix} = \sigma \begin{bmatrix} m \\ n \end{bmatrix}, \ \mathrm{mod} N,$$

$$\begin{bmatrix} m_t \\ n_t \end{bmatrix} = \tau \begin{bmatrix} m \\ n \end{bmatrix}, \ \mathrm{mod} N,$$

The realization of $(C_N \times C_N) \leftthreetimes (C_2 \times C_2)$ with σ and τ is given by

$$(a^m b^n)^\sigma \longrightarrow a^{m_s} b^{n_s}, \quad (a^m b^n)^\tau \longrightarrow a^{m_t} n_t.$$

The affine realizations are based on the homogeneous coordinate system. For a 2×2 matrix σ of order 2, associate the matrices

$$\sigma_{i,j} = \begin{bmatrix} s_1 & s_2 & i\frac{N}{2} \\ s_3 & s_4 & j\frac{N}{2} \\ 0 & 0 & 1 \end{bmatrix}, \quad 0 \leq i, j \leq 1.$$

$\sigma_{i,j}$ is of order 2 and acts as an affine motion on $(m,n) \in \mathbf{Z}/N \times \mathbf{Z}/\mathbf{N}$ through the matrix multiplication

$$\sigma_{i,j} \begin{bmatrix} m \\ n \\ 1 \end{bmatrix}, \quad 0 \leq i, j \leq 1.$$

5.2 Code development for successive processing

In general, the results of successively processing an image by projection operators associated with two distinct realizations of an abstract group are distinct. Moreover, the order in which the projections are applied results in significant differences in the resulting image.

One framework for predictable, successive processing is developed by constructing two realizations $A \wr B$ and $A \wr C$ such that B and C commute. In the case of $G = (C_N \times C_N) \wr (C_2 \times C_2)$, if the two realizations of G are obtained from 4 commuting matrices representing the four copies of C_2's, then the projections are not affected by the order of processing, and the discriminating characteristics are predictable. The discriminating properties of the resulting projections are equivalent to processing by the projection operators associated with the much larger group $(C_N \times C_N) \wr (C_2 \times C_2 \times C_2 \times C_2)$.

Example: Two commuting realizations

The following 4 elements commute and generate a 16-group.

$$\overset{a}{\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}}, \quad \overset{b}{\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}}, \quad \overset{c}{\begin{bmatrix} \frac{N}{2} & \frac{N}{2}-1 \\ \frac{N}{2}-1 & \frac{N}{2} \end{bmatrix}}, \quad \overset{d}{\begin{bmatrix} 0 & \frac{N}{2}-1 \\ \frac{N}{2}-1 & 0 \end{bmatrix}}.$$

All the distinct centralizers are realized by successively processing with $A = (C_N \times C_N) \wr (a \times b)$ and $B = (C_n \times C_n) \wr (c \times d)$. Projections are distinguished by the distinct subgroups of $a \times b$ and $c \times d$. In terms of imaging characteristics, these projections distinguish the same projections as the subgroups of the group generated by all four elements. However, the order of the distinguishing subgroups determine the dimensionality of the invariant subspaces and affects the detectability as opposed to discrimination.

We have investigated and identified the relevant image processing properties of many realizations based on the following MATLAB codes.

- codes generating exhaustive set of realizations,
- codes constructing complete set of primitive idempotents,
- codes constructing unitary transformations from complete set of primitive idempotents,
- codes implementing varying filters in the spectral domain.

6 Implementation results

All figures in this report are log-scaled, gray-scale intensity plots.

6.1 Classifying geometric properties

6.1.1 Realizations of $(C_N \times C_N) \not\wr (C_2 \times C_2)$

Filters identifying lines at varying orientations

Large collection of filters that distinguish lines at varying orientations have been implemented. For digital implementation, orientations are described by varying slopes. For the selected realizations we chose, it is possible to distinguish between lines which differ in slopes of $\frac{1}{N}$. For a large N, this translates to small angular differences.

Filters composed of 2-dimensional idempotents discriminate lines of slopes 1 and -1.

$$A_{11} = \left\{ a_0 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad a_{11} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad a_0 a_{11} = a_{11} a_0, = \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}.$$

Figure 6.1.1

Figure 6.1.2

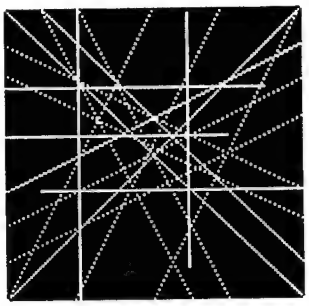


Figure 6.1.3

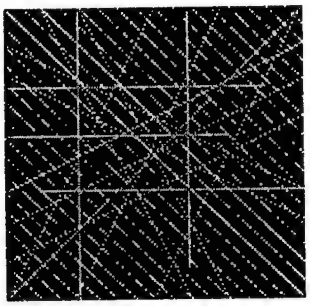


Figure 6.1.4

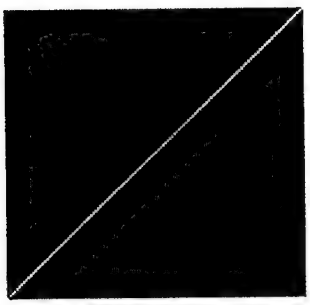


Figure 6.1.5

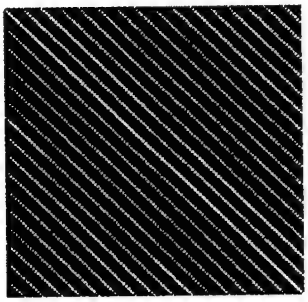


Figure 6.1.6

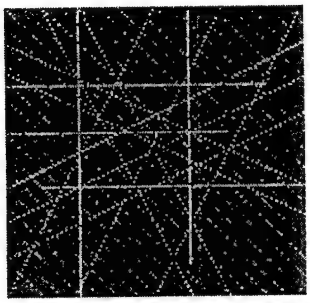


Figure 6.1.1. Random intensity between 0–10 along lines of slope -1.

Figure 6.1.2. Several lines of maximum intensity 5.

Figure 6.1.3. Sum of intensities in Figures 1.1 and 1.2 which is the input to the nonabelian filters.

Figures 6.1.4 and 6.1.5. Results of filtering by 2 of the 2-dimensional idempotents.

Figure 6.1.6. Result of filtering by the 4-dimensional idempotents.

Performance of the 2-dimensional idempotents of $\mathbf{C}\left((C_N \times C_N) \leftthreetimes (C_2 \times C_2)\right)$ in noise.

Figure 6.2.1

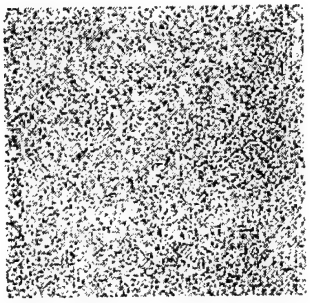


Figure 6.2.2

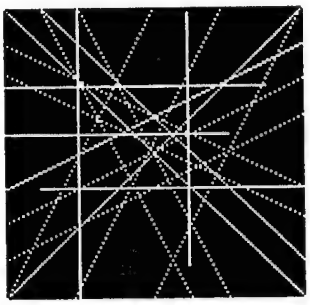


Figure 6.2.3

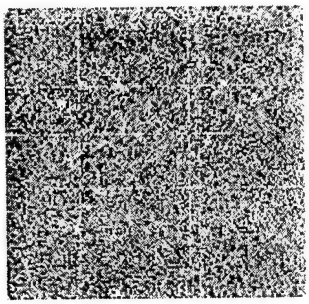


Figure 6.2.4

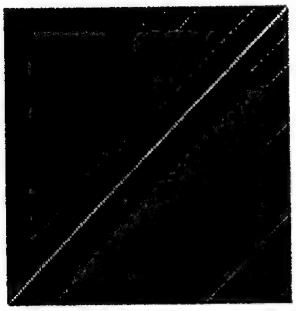


Figure 6.2.5

Figure 6.2.1. Random noise of variance 15 and zero mean.

Figure 6.2.2. Several lines of maximum intensity 5.

Figure 6.2.3. Sum of intensities in Figures 2.1 and 2.2 which is the input to the nonabelian filters.

Figures 6.2.4 and 6.2.5. Results of filtering by 2 of the 2-dimensional idempotents.

Filters composed of 2-dimensional idempotents discriminate lines of slopes -2 and 0.

$$A_{13} = \left\{ a_0 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad a_{13} = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}, \quad a_0 a_{13} = a_{13} a_0 = \begin{bmatrix} -1 & -1 \\ 0 & 1 \end{bmatrix} \right\}.$$

Figure 6.3.1

Figure 6.3.2

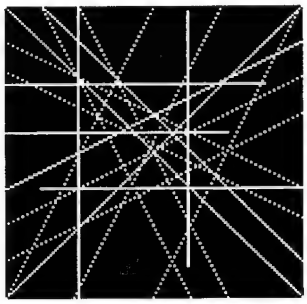


Figure 6.3.3

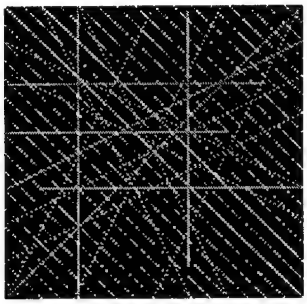


Figure 6.3.4

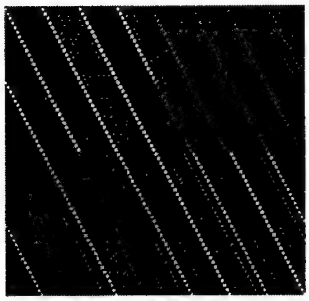


Figure 6.3.5

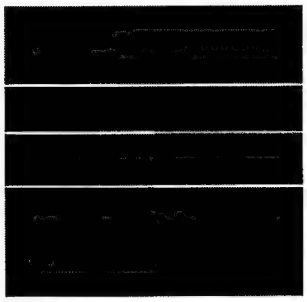


Figure 6.3.6

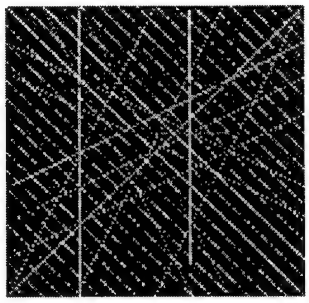


Figure 6.3.1. Random intensity between 0–10 along lines of slope -1.

Figure 6.3.2. Several lines of maximum intensity 5.

Figure 6.3.3. Sum of intensities in Figures 6.3.1 and 6.3.2 which is the input to the nonabelian filters.

Figures 6.3.4 and 6.3.5. Results of filtering by 2 of the 2-dimensional idempotents.

Figure 6.3.6. Result of filtering by the 4-dimensional idempotents.

Filters identifying varying periodic structures

Checkerboard pattern is projected onto 1-dimensional idempotents.

$$A = \left\{ I_2, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} \right\}.$$

Figure 6.4.1

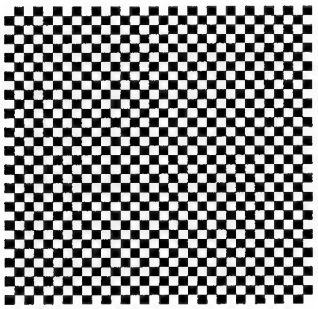


Figure 6.4.2

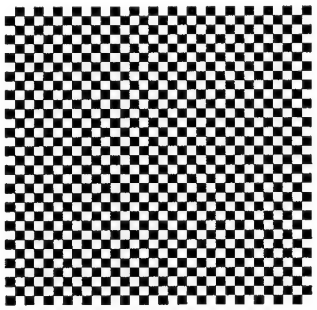


Figure 6.4.1. 32×32 alternating intensities of 0 and 1.

Figure 6.4.2. The result of filtering by 1-dimensional idempotents.

Figure 6.4.3

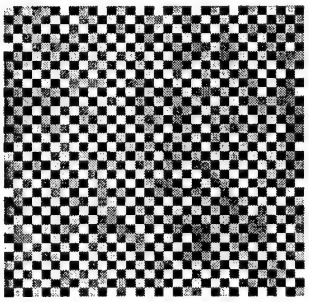


Figure 6.4.4

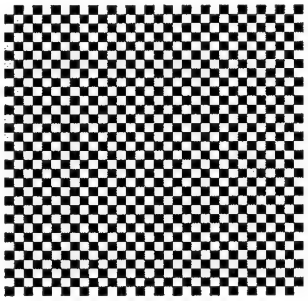


Figure 6.4.5

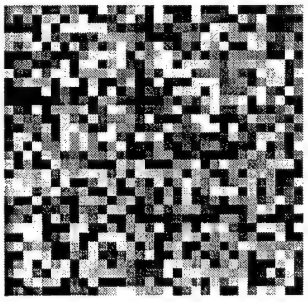


Figure 6.4.3. Random noise of variance 1 and norm 16.19 is added to the checkerboard pattern in Figure 6.4.1, and used as the input to filters generated by the group A. The norm of the composite image is 32.12.

Figure 6.4.4. The result of filtering by 1-dimensional idempotents.

Figure 6.4.5. The result of filtering by 4-dimensional idempotents.

Checkerboard pattern with detail is projected into the 1-dimensional idempotents and first of the three 2-dimensional idempotents.

$$B = \left\{ I_2, \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \frac{N}{2}-1 \\ \frac{N}{2}-1 & 0 \end{bmatrix}, \begin{bmatrix} \frac{N}{2}+1 & 0 \\ 0 & \frac{N}{2}+1 \end{bmatrix} \right\}.$$

Figure 6.5.1

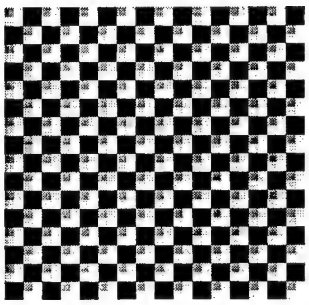


Figure 6.5.2

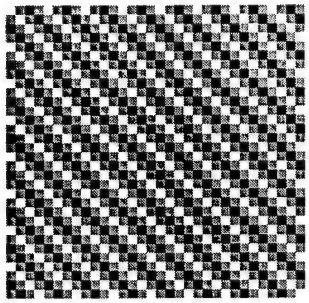


Figure 6.5.3

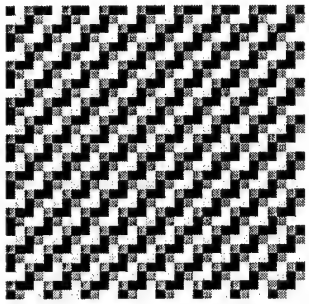


Figure 6.5.1. Input image of 32×32 checkerboard pattern is made up of 2×2 squares of intensities 2, 3 and 4.

Figure 6.5.2. Result of filtering by 1-dimensional idempotents.

Figure 6.5.3. Result of filtering by the first of the three 2-dimensional idempotents.

Figure 6.5.4

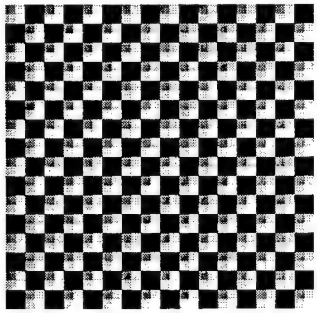


Figure 6.5.4. Sum of the intensities of images in Figures 6.5.2 and 6.5.3.

Performance of these filters are tested in noise.

Figure 6.5.5 Figure 6.5.6 Figure 6.5.7

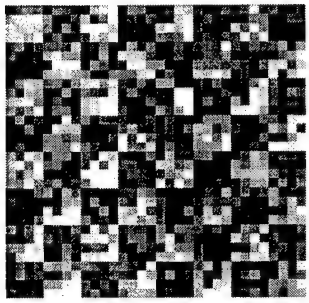
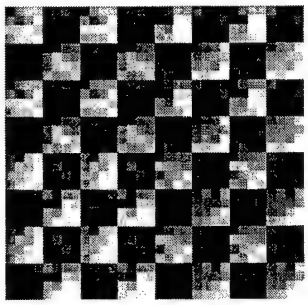
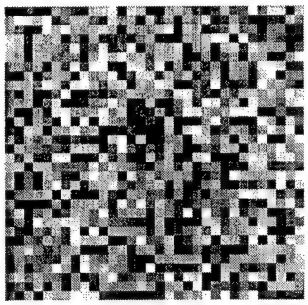




Figure 6.5.5. Random noise of values 0–4 is added to the checkerboard pattern of Figure 6.5.1 to form the input image.

Figure 6.5.6. The sum of the results of filtering by 1-dimensional idempotents and the first of the three 2-dimensional idempotents.

Figure 6.5.7. The result of filtering by the 4-dimensional idempotents.

Checkerboard pattern with detail is projected into the 1-dimensional idempotents and second of the three 2-dimensional idempotents.

$$C = \left\{ I_2, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \frac{N}{2}+1 \\ \frac{N}{2}+1 & 0 \end{bmatrix}, \begin{bmatrix} \frac{N}{2}+1 & 0 \\ 0 & \frac{N}{2}+1 \end{bmatrix} \right\}.$$

Figure 6.6.1

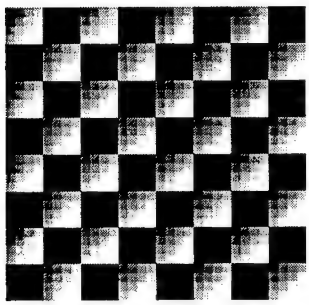


Figure 6.6.2

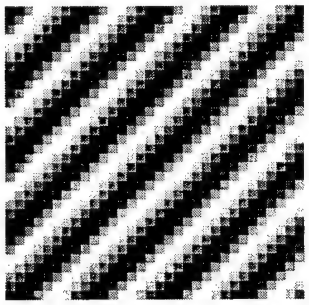


Figure 6.6.3

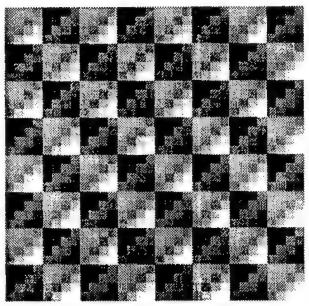


Figure 6.6.1. Input image of 32×32 is made up of 4×4 squares of intensities of integer values 2–8.

Figure 6.6.2. Result of filtering by 1-dimensional idempotents.

Figure 6.6.3. Result of filtering by the second of the three 2-dimensional idempotents.

Figure 6.6.4

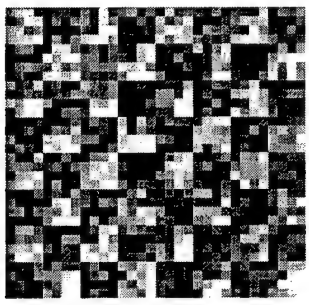


Figure 6.6.5

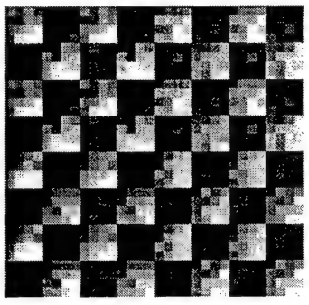


Figure 6.6.6

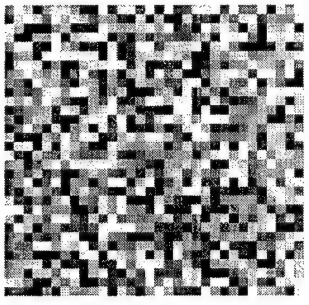


Figure 6.6.4. Input image of 32×32 is generated by adding random noise of intensities 0–8 to the image in Figure 6.6.1.

Figure 6.6.5. The sum of results of filtering by 1-dimensional idempotents and the second of the 2-dimensional idempotents.

Figure 6.6.6. Result of filtering by the 4-dimensional idempotents.

Periodic structure is projected into the second of the three 2-dimensional idempotents.

$$D = \left\{ I_2, \begin{bmatrix} -1 & 0 & \frac{N}{2} \\ 0 & -1 & \frac{N}{2} \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & -1 & \frac{N}{2} \\ -1 & 0 & \frac{N}{2} \\ 0 & 0 & 1 \end{bmatrix} \right\}.$$

Figure 6.7.1

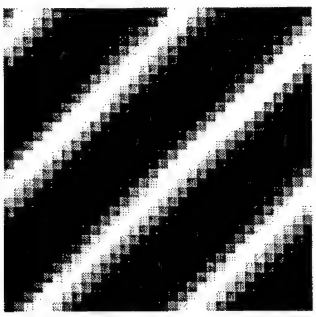


Figure 6.7.1. Image of 32×32 of intensity 0–4.

Figure 6.7.2

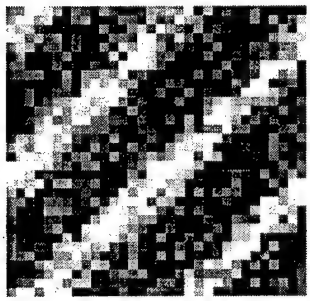


Figure 6.7.3

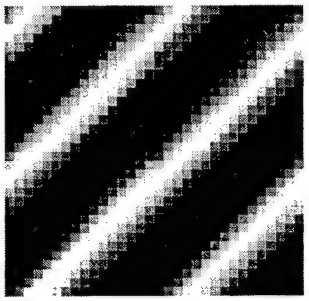


Figure 6.7.4

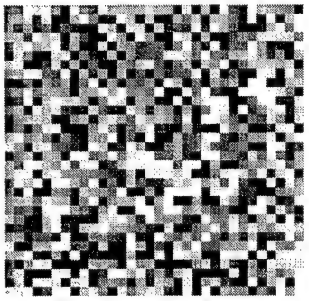


Figure 6.7.2. Input image of 32×32 is generated by adding random intensities of 0–4 to the image in Figure 7.1.

Figure 6.7.3. The result of filtering by the second of the 2-dimensional idempotents.

Figure 6.7.4. Result of filtering by the 4-dimensional idempotents.

Periodic pattern is projected into the second of the three 2-dimensional idempotents.

Figure 6.8.1

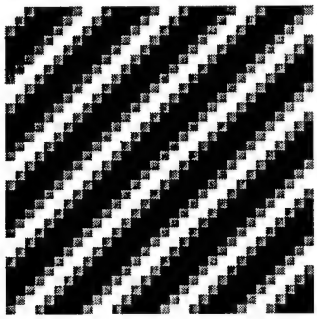


Figure 6.8.1. Image of 32×32 of intensity 0–2.

Figure 6.8.2

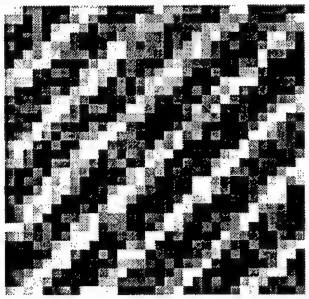


Figure 6.8.2. Input image of 32×32 is generated by adding random noise of intensities 0–4 to the image in Figure 7.5.

Figure 6.8.3

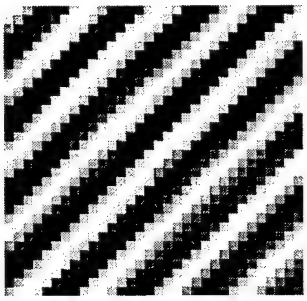


Figure 6.8.3. The result of filtering by the second of the 2-dimensional idempotents.

Figure 6.8.4

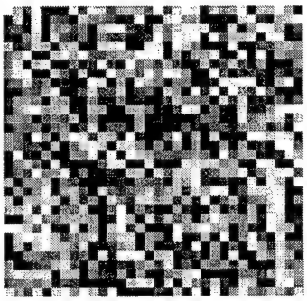


Figure 6.8.4. Result of filtering by the 4-dimensional idempotents.

6.1.2 Realizations of $(C_N \times C_N) \leftthreetimes C_4$

Numerical experiments included in this section illustrate the image processing characteristics of the varying realizations of $(C_N \times C_N) \leftthreetimes C_4$. Robustness of these properties are tested in random white noise.

Figure 6.9.1

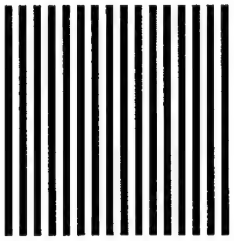


Figure 6.9.2

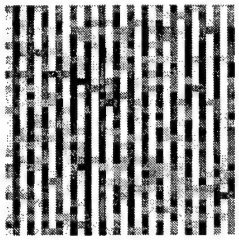


Figure 6.9.3

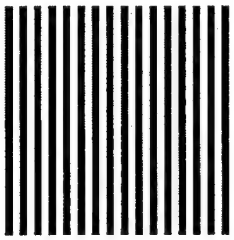
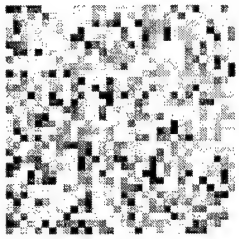


Figure 6.9.4



White noise of zero mean and standard deviation of 50% of maximum intensity is added to the image in Figure 9.1 to generate the input image in Figure 6.9.2.

Figure 6.9.3. The result of projections by lower dimensional idempotents.

Figure 6.9.4. The residual.

Figure 6.10.1

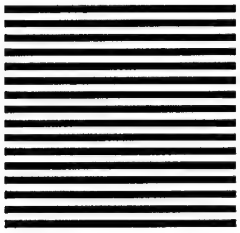


Figure 6.10.2

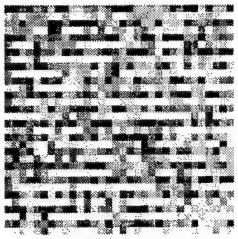


Figure 6.10.3

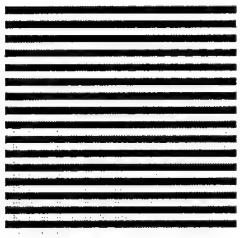
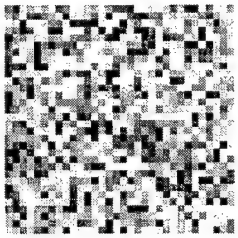


Figure 6.10.4



White noise of zero mean and standard deviation of maximum intensity is added to the image in Figure 6.10.1 to generate the input image in Figure 6.10.2.

Figure 6.10.3. The result of projections by lower dimensional idempotents.

Figure 6.10.4. The residual.

Figure 6.11.1

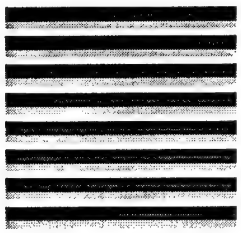


Figure 6.11.2

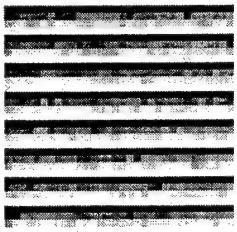


Figure 6.11.3

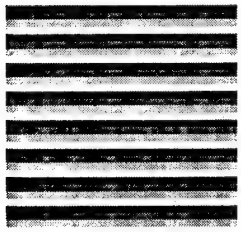
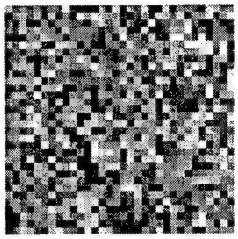


Figure 6.11.4



White noise of zero mean and standard deviation of 20% of the maximum intensity is added to the image in Figure 11.1 to generate the input image in Figure 6.11.2.

Figure 6.11.3. The result of projections by lower dimensional idempotents.

Figure 6.11.4. The residual.

Figure 6.12.1 Figure 6.12.2 Figure 6.12.3

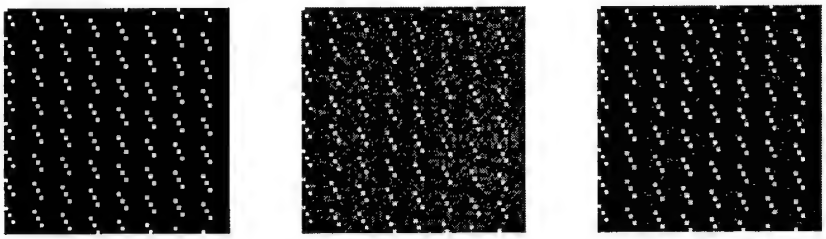


Figure 6.12.4 Figure 6.12.5 Figure 6.12.6

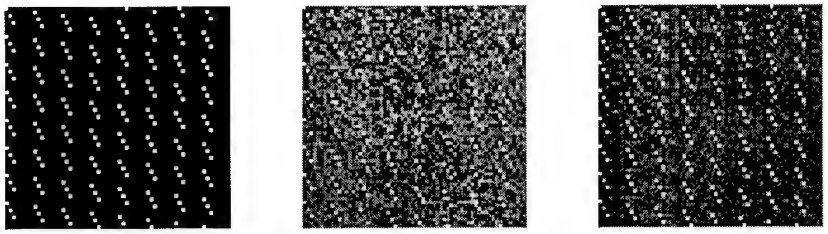
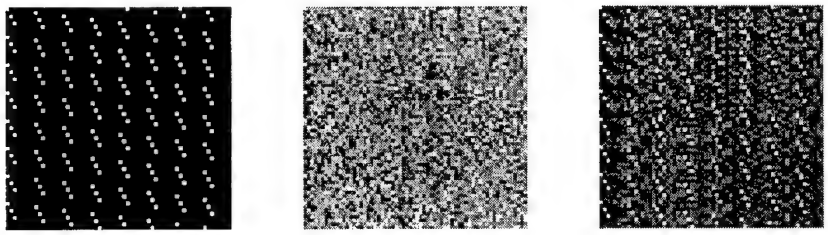


Figure 6.12.7 Figure 6.12.8 Figure 6.12.9



White noise of zero mean and standard deviation of 50% of the maximum intensity is added to the image in Figure 6.12.1 to generate the input image in Figure 6.12.2.

Figure 6.12.3. The projection by lower dimensional idempotents.

White noise of zero mean and standard deviation of the maximum intensity is added to the image in Figure 6.12.4 to generate the input image in Figure 6.12.5.

Figure 6.12.6. The result of projection by lower dimensional idempotents.

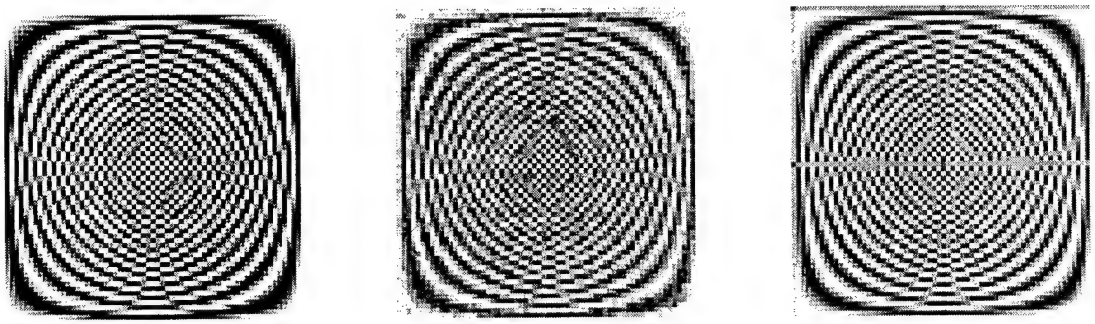
White noise of zero mean and standard deviation of 150% of the maximum intensity is added to the image in Figure 6.12.7 to generate the input image in Figure 6.12.8.

Figure 6.12.9. The projection by lower dimensional idempotents.

6.2 Extending the library

To extend the library of projections discriminating prescribed geometry, we have implemented the convolution and projection algorithms associated with groups that operate on spaces that are unitarily equivalent to the image space. These include in particular, the spaces of one and two-dimensional frequencies.

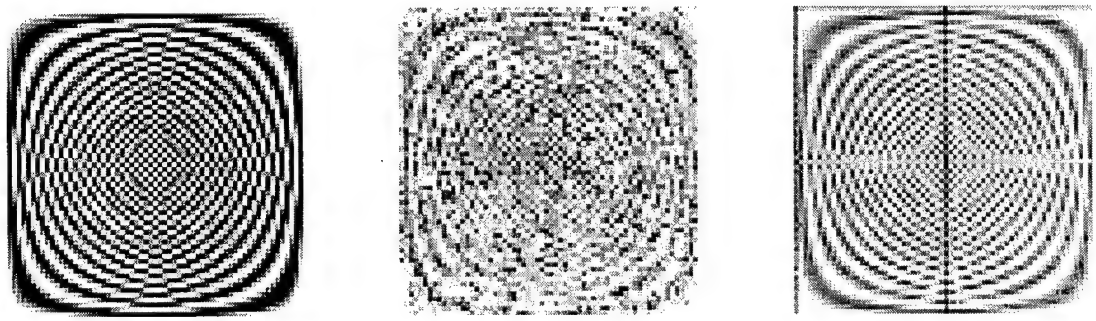
Figure 6.13.1 Figure 6.13.2 Figure 6.13.3



White noise of zero mean and standard deviation of 100% of maximum intensity is added to the image of size 64 × 64 in Figure 6.13.1 to generate the input image in Figure 6.13.2.

Figure 6.13.3 is the result of nonabelian group projection discriminating periodicity in frequency.

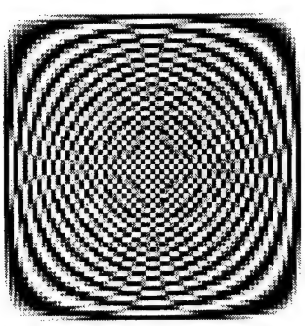
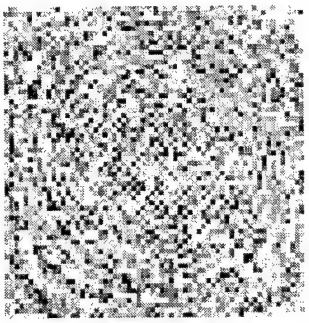
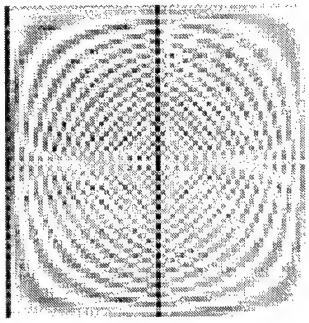
Figure 6.14.1 Figure 6.14.2 Figure 6.14.3



White noise of zero mean and standard deviation of 300% of maximum intensity is added to the image of size 64 × 64 in Figure 6.14.1 to generate the input image in Figure 6.14.2.

Figure 6.14.3 is the result of nonabelian group projection discriminating periodicity in frequency.

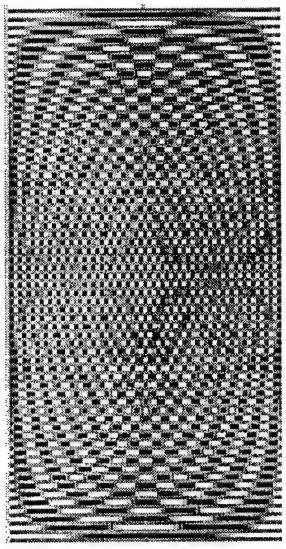
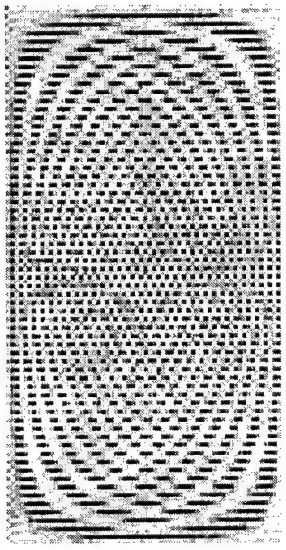
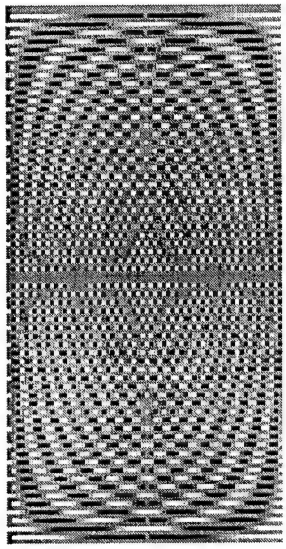
Figure 6.15.1 Figure 6.15.2 Figure 6.15.3

White noise of zero mean and standard deviation of 500% of maximum intensity is added to the image of size 64×64 in Figure 6.15.1 to generate the input image in Figure 6.15.2.

Figure 6.15.3 is the result of nonabelian group projection discriminating periodicity in frequency.

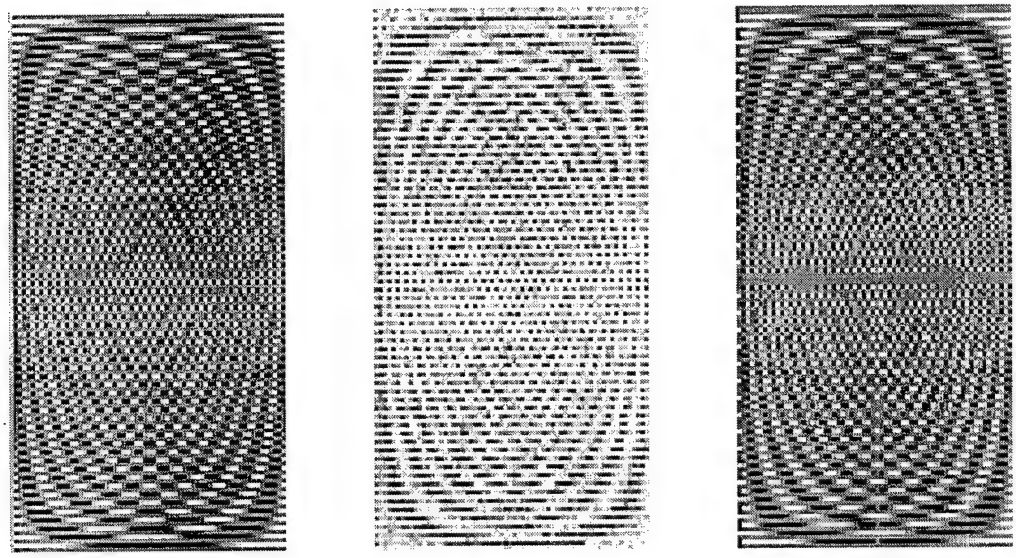
Figure 6.16.1 Figure 6.16.2 Figure 6.16.3

White noise of zero mean and standard deviation of 100% of maximum intensity is added to the image of size 128×128 in Figure 6.16.1 to generate the input image in Figure 6.16.2.

Figure 6.16.3 is the result of nonabelian group projection discriminating periodicity in frequency.

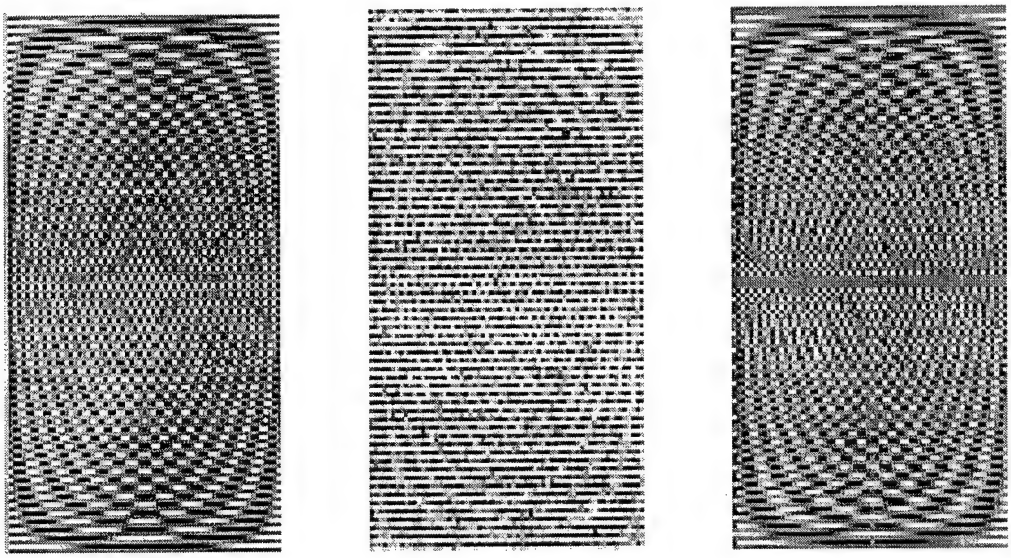
Figure 6.17.1 Figure 6.17.2 Figure 6.17.3



White noise of zero mean and standard deviation of 300% of maximum intensity is added to the image of size 128×128 in Figure 6.17.1 to generate the input image in Figure 6.17.2.

Figure 6.17.3 is the result of nonabelian group projection discriminating periodicity in frequency.

Figure 6.18.1 Figure 6.18.2 Figure 6.18.3



White noise of zero mean and standard deviation of 500% of maximum intensity is added to the image of size 128×128 in Figure 6.18.1 to generate the input image in Figure 6.18.2.

Figure 6.18.3 is the result of nonabelian group projection discriminating periodicity in frequency.

6.3 Software design tool

The library of codes implementing nonabelian group convolutions and projections is extensive. For image data consisting of intensities, the filters implemented in the projection domain respects this information. The result of such filtering is an image data of similar characteristics, allowing successive and iterative processing. By combining several projections and filters, extensive and non-traditional image segmentation is possible.

6.3.1 Segmentation by spatial periodicity

Figure 6.19.1

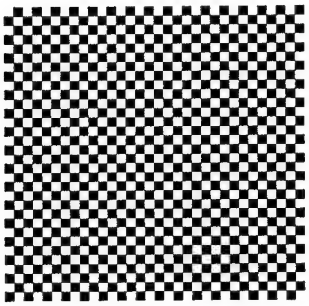


Figure 6.19.2

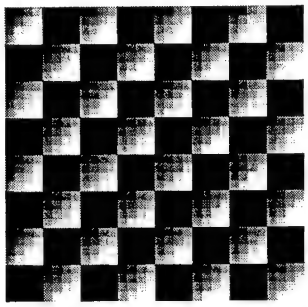


Figure 6.19.3

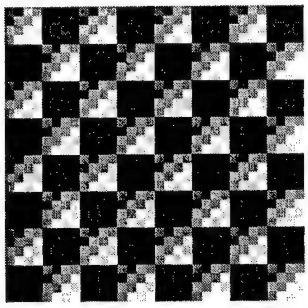


Figure 6.19.1. Image of 32×32 of alternating intensity of 0 and 2.

Figure 6.19.2. Image of 32×32 checkerboard pattern made up of 2×2 squares of intensities 2–5.

Figure 6.19.3. The sum of the intensities in Figures 6.19.1 and 6.19.2 is used as input for analysis.

Figure 6.19.4

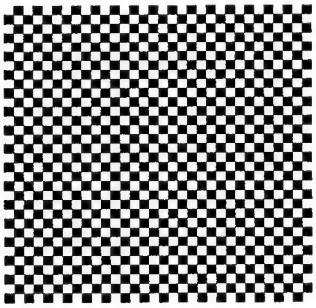


Figure 6.19.5

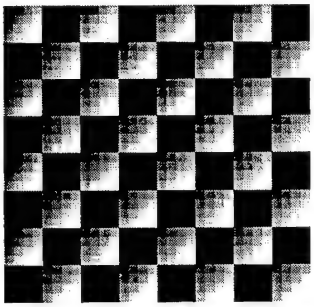


Figure 6.19.4. The result of projecting the image in Figure 6.19.1.

Figure 6.19.5. The sum of the results of projecting the residual.

Figure 6.19.7

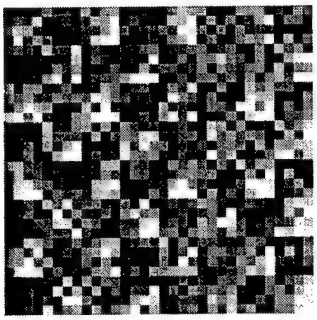


Figure 6.19.8

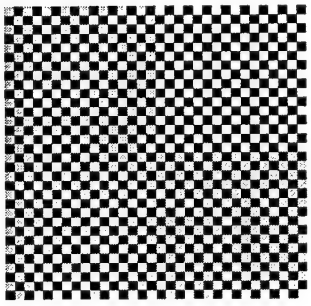


Figure 6.19.9

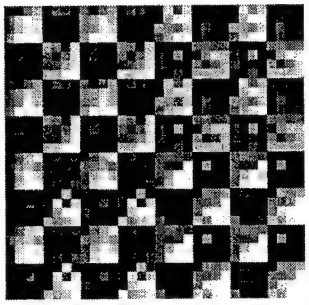


Figure 6.19.10

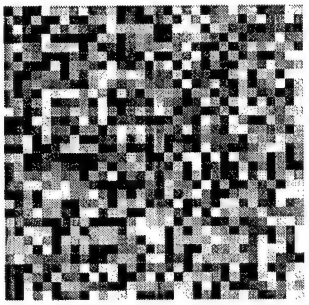


Figure 6.19.7. Randomized intensity of 0–10 added to the image in Figure 6.19.3.

Figure 6.19.8. The result of projecting the image in Figure 6.19.7.

Figure 6.19.9. The sum of the results of projecting the residual.

Figure 6.19.10. The residual.

Figure 6.20.1

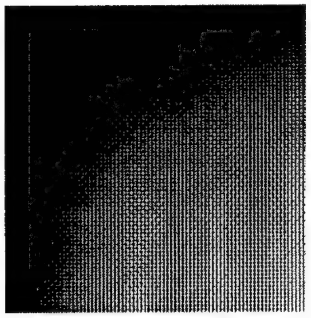


Figure 6.20.2

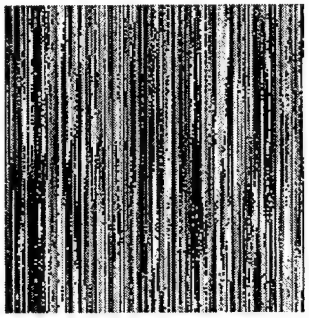


Figure 6.20.3

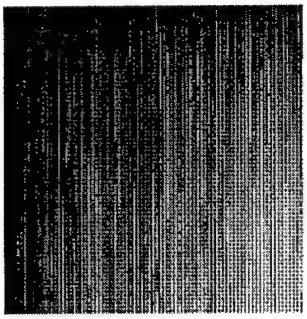


Figure 6.20.4

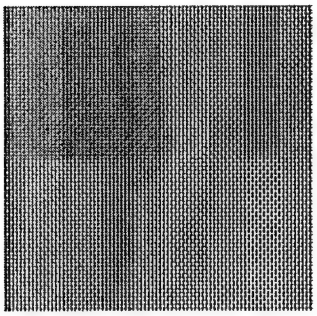


Figure 6.20.5

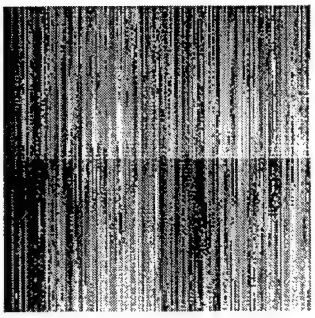


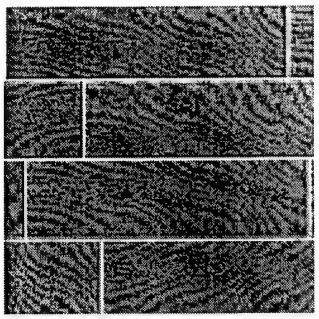
Figure 6.20.1. Simulated checkerboard pattern of size 160×160.

Figure 6.20.2. Downloaded web image of size 160×160.

Figure 6.20.3. Sum of images in Figures 6.20.1 and 6.20.2. is used as an input to processing.

Figures 6.20.4, 6.20.5. Results of projection.

Figure 6.21.1



Downloaded web image of six 256 × 256.

Figure 6.21.2

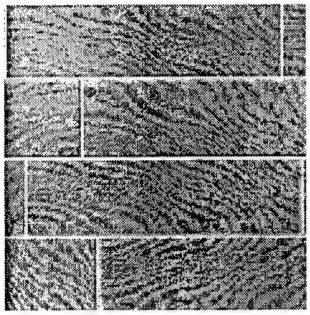


Figure 6.21.3

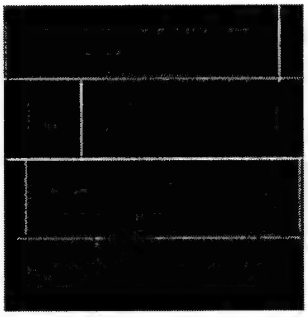


Figure 6.21.4

Figure 6.21.2. White noise is added to the image in Figure 6.21.1 to generate the input image to processing.

Figures 6.21.3 and 6.21.4. Results of projections discriminating lines of distinct orientations and sizes.

Figure 6.21.5 Figure 6.21.6 Figure 6.21.7

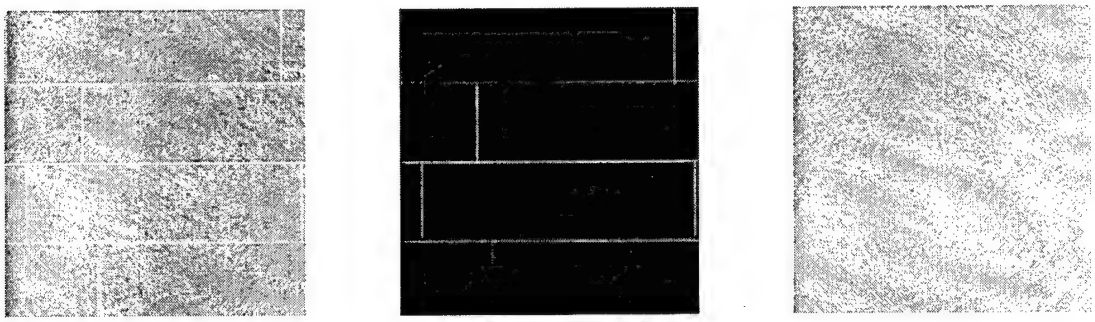


Figure 6.21.5. White noise is added to the image in Figure 6.21.1 to generate the input image to processing.

Figures 6.21.6 and 6.21.7. Results of projections discriminating lines of distinct orientations and sizes.

Figure 6.21.8 Figure 6.21.9 Figure 6.21.10

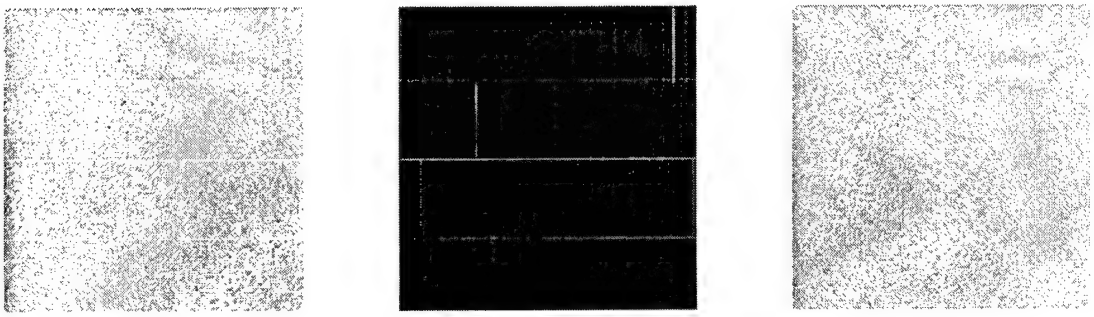


Figure 6.21.6. White noise is added to the image in Figure 6.21.1 to generate the input image to processing.

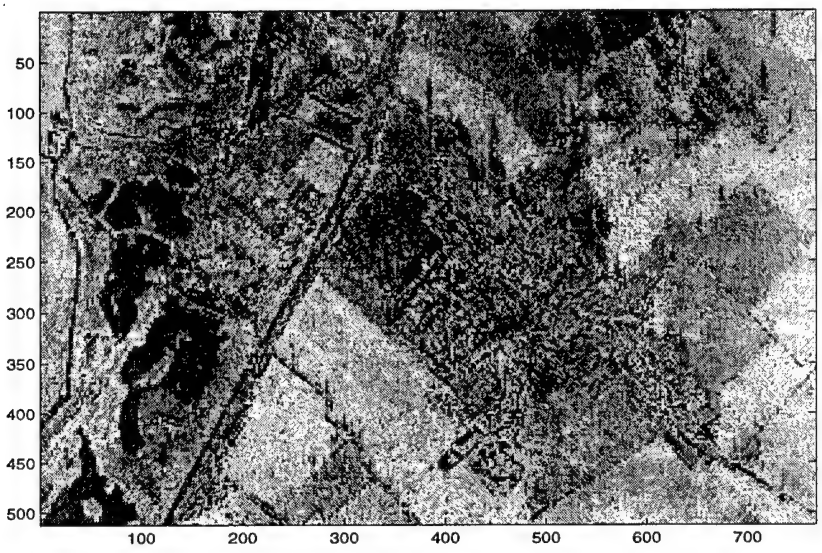
Figures 6.21.9 and 6.21.10. Results of projections discriminating lines of distinct orientations and sizes.

7 Design Examples

7.1 Example: image segmentation

SAR image off the web is segmented in two distinct ways.

Figure 7.1.1



Download web image of *Stanwick*.

7.1.1 Image segmentation by spatially varying projections

The projections are constructed from the 1-dimensional idempotents of $(C_N \times C_N) \wr C_4$.

Figure 7.1.2

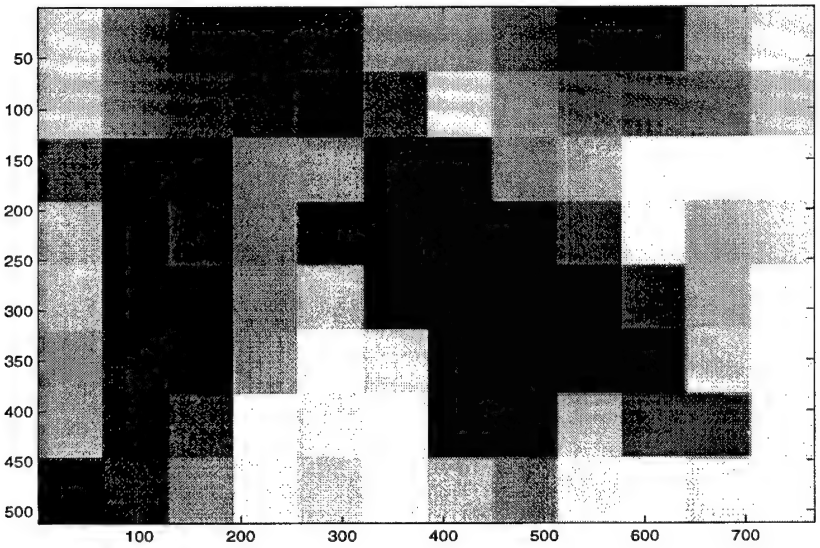


Figure 7.1.3

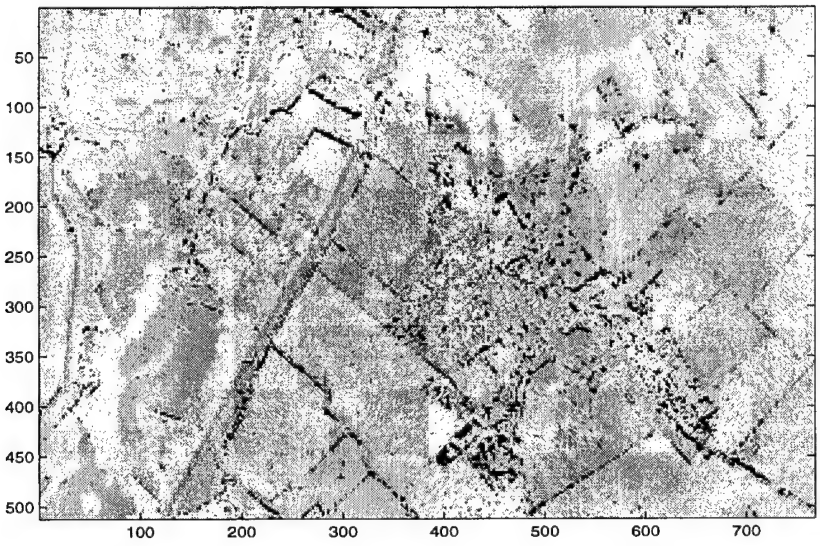


Figure 7.1.2. The result of applying the spatially varying projection constructed from 1-dimensional idempotents of one of the realizations of $(C_N \times C_N) \wr C_4$.

Figure 7.1.3. The residual.

7.1.2 Image segmentation by textural differences

The projections are constructed from the 2-dimensional idempotents of $(C_N \times C_N) \leftthreetimes C_4$.

Figure 7.1.4

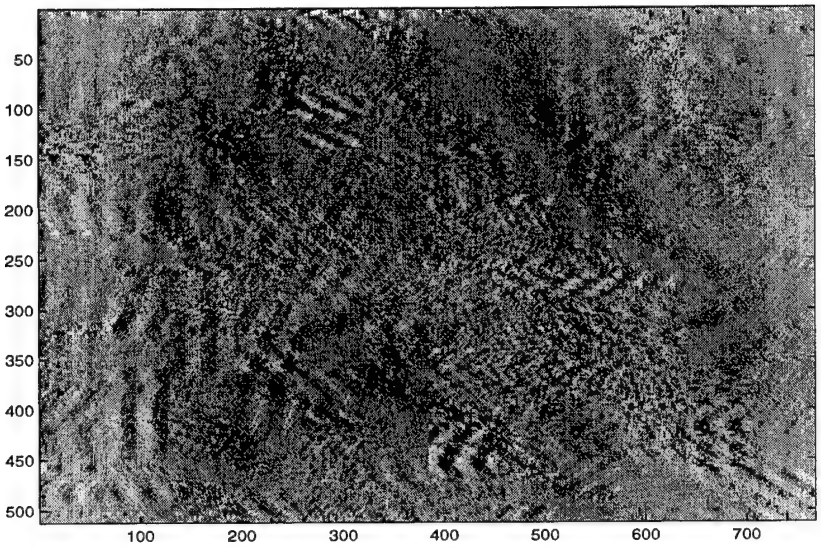


Figure 7.1.5

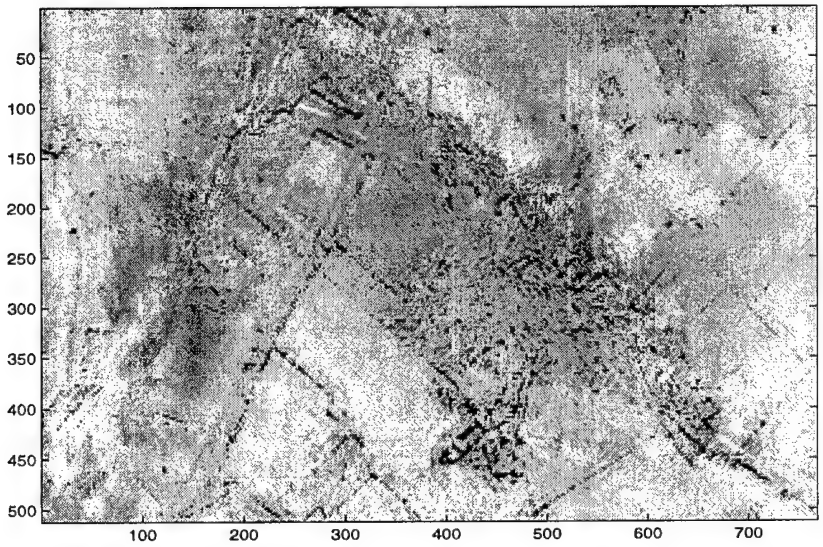
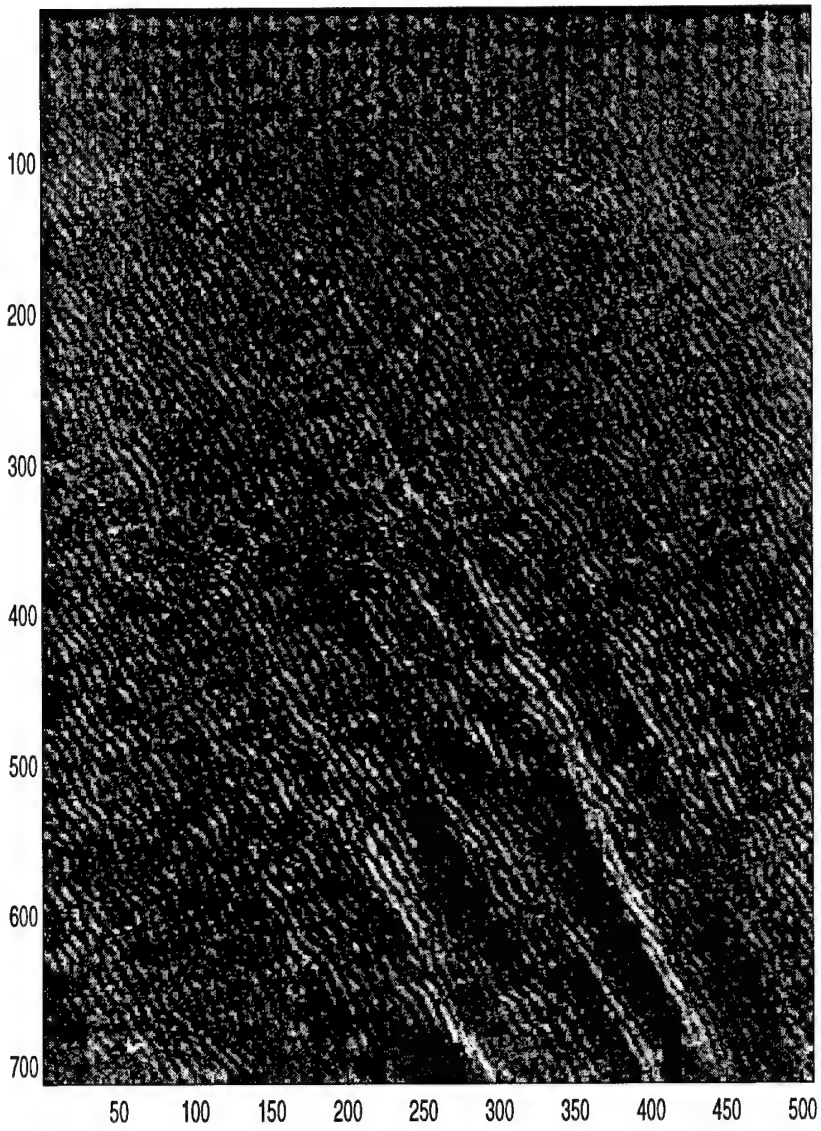


Figure 7.1.4. The result of applying the projection discriminating textural (periodic) information constructed from 2-dimensional idempotents of one of the realizations of $(C_N \times C_N) \leftthreetimes C_4$.

Figure 7.1.5. The residual.

Sidescan sonar image is segmented by textural differences.

Figure 7.1.6



Sidescan sonar image of ocean floor.

Figure 7.1.7

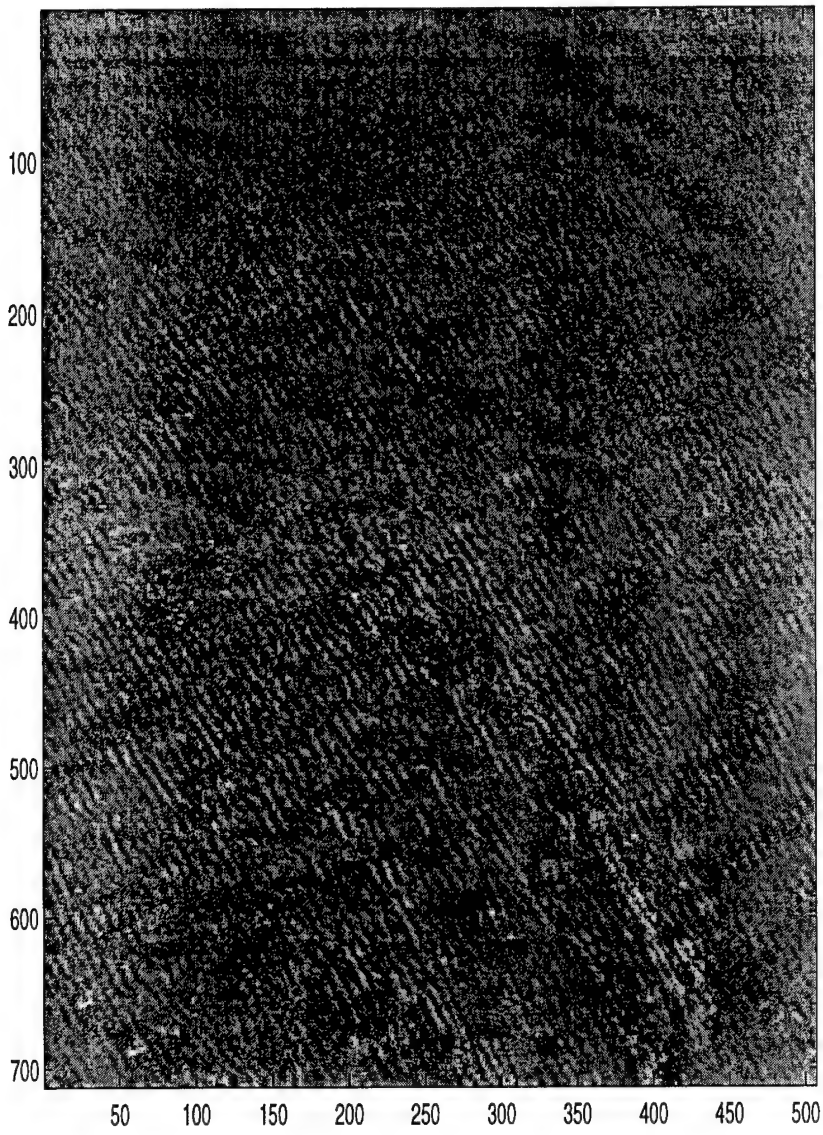

100
200
300
400
500
600
700
50
100
150
200
250
300
350
400
450
500

Figure 7.1.8

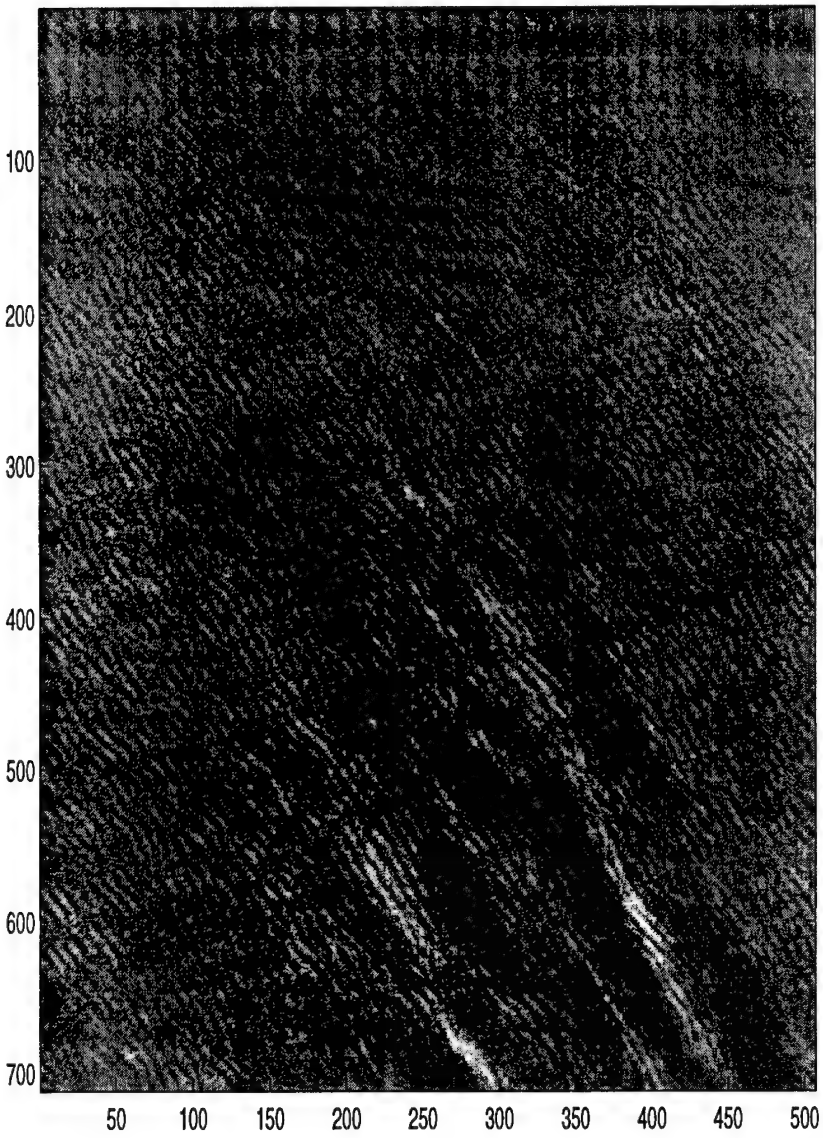


Figure 7.1.7. The result of applying the projection discriminating textural (periodic) information constructed from 2-dimensional idempotents of one of the realizations of $(C_N \times C_N) \rtimes C_4$.

Figure 7.1.8. The residual.

7.2 Software tool for automatic pattern localization

Codes implementing detection of prescribed patterns have been developed to locate the position of the patterns. Unlike the traditional methods based on matched filtering, the nonabelian projection methods can detect and locate patterns of abstract descriptions that are independent of variances in scale and magnitude of the patterns.

Encoding of prescribed pattern into an invariant subspace is a design process, based on selection of a nonabelian group. Once this encoding is completed however, locating the pattern is automatic.

A pattern that can be encoded into an invariant subspace is embedded into various backgrounds. The nonabelian group chosen for the example is one realization of the abstract group $G = (C_N \times C_N) \nleftarrow (C_2 \times C_2)$,

$$C_2 \times C_2 \sim \left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix} \right).$$

The operator which projects an image into the selected invariant subspace *partitions* the image within the projection (depending on the location of the encoded pattern and the background) into quadrants, by 4 levels of magnitudes, by the action of $C_2 \times C_2$. We have used the relative levels of magnitudes of the quadrants to determine the *amount* of the prescribed pattern occupying the quadrants. From the knowledge of the relative size of the prescribed pattern, off-set location is determined successively. Current implementation requires 4 iterations. The number of iterations depend largely on the extent of the pattern: The larger the pattern, the fewer the iteration. At each iteration, the test data size is reduced by 50%. The computational complexity of each iteration is in the order of $2N\log N$, where N is the test data size.

The current implementation is parameterized for N, a power of 2, which determines the data size, $2N \times 2N$ and the size of the pattern is set at $\frac{N}{2} \times \frac{N}{2}$.

7.2.1 Example scenes

Location of horizontal bars in random background

Figure 7.2.1

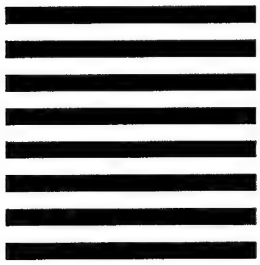


Figure 7.2.2

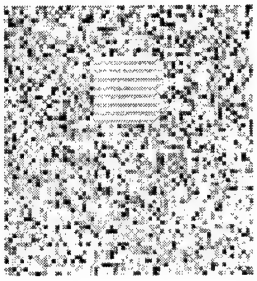


Figure 7.2.3

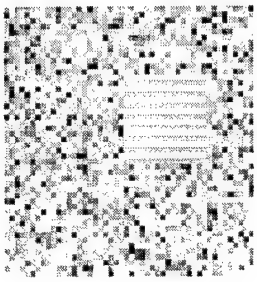


Figure 7.2.4

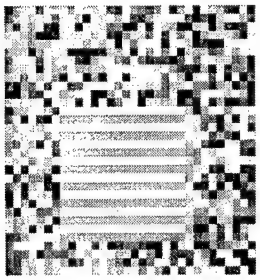


Figure 7.2.5

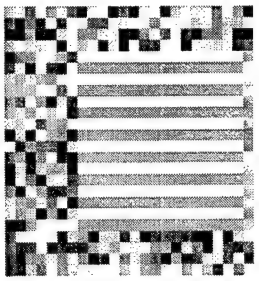


Figure 7.2.6

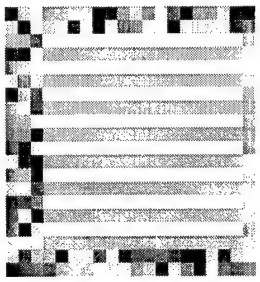


Figure 7.2.1. Pattern of alternating horizontal bars of size 16×16.

Figure 7.2.2. Pattern in Figure 3.1 is placed in the scene of randomized magnitude of size 64×64. The placement is chosen randomly.

Figure 7.2.3. Based on the result of the first iteration of the projection of off-set coordinate of $(0, 0)$, the test image on coordinates $[0 : 47, 0 : 47]$ is displayed.

Figure 7.2.4. Based on the result of the second iteration of the projection of off-set coordinate of $(0, 16)$, the test image on coordinates $[0 : 31, 16 : 47]$ is displayed .

Figure 7.2.5. Based on the result of the second iteration of the projection of off-set coordinate of $(8, 16)$, the test image on coordinates $[8 : 31, 16 : 39]$ is displayed .

Figure 7.2.6. Based on the result of the second iteration of the projection of off-set coordinate of $(10, 20)$, the test image on coordinates $[10 : 29, 20 : 39]$ is displayed.

Location of noisy horizontal bars in random background

Figure 7.3.1 Figure 7.3.2 Figure 7.3.3

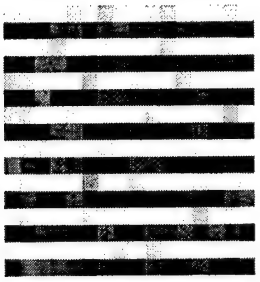
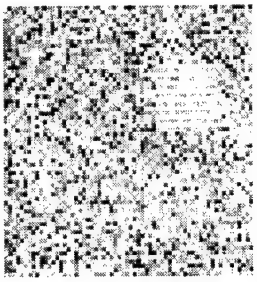
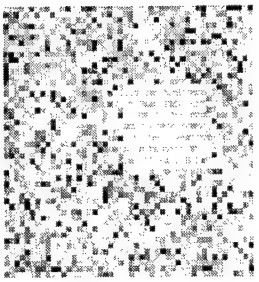




Figure 7.3.4 Figure 7.3.5 Figure 7.3.6

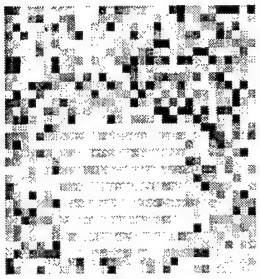
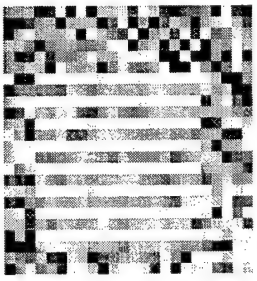
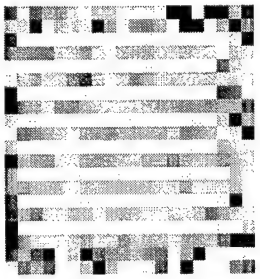




Figure 7.3.1. Pattern of alternating noisy horizontal bars of size 16×16.

Figure 7.3.2. Pattern in Figure 4.1 is placed in the scene of randomized magnitude of size 64×64. The placement is chosen randomly.

Figure 7.3.3. Based on the result of the first iteration of the projection of off-set coordinate of $(0, 16)$, the test image on coordinates $[0 : 47, 16 : 63]$ is displayed.

Figure 7.3.4. Based on the result of the second iteration of the projection of off-set coordinate of $(0, 32)$, the test image on coordinates $[0 : 31, 32 : 63]$ is displayed .

Figure 7.3.5. Based on the result of the second iteration of the projection of off-set coordinate of $(8, 36)$, the test image on coordinates $[8 : 31, 36 : 59]$ is displayed .

Figure 7.3.6. Based on the result of the second iteration of the projection of off-set coordinate of $(12, 38)$, the test image on coordinates $[12 : 31, 38 : 57]$ is displayed.

Location of horizontal bars in random background

Figure 7.4.1 Figure 7.4.2 Figure 7.4.3

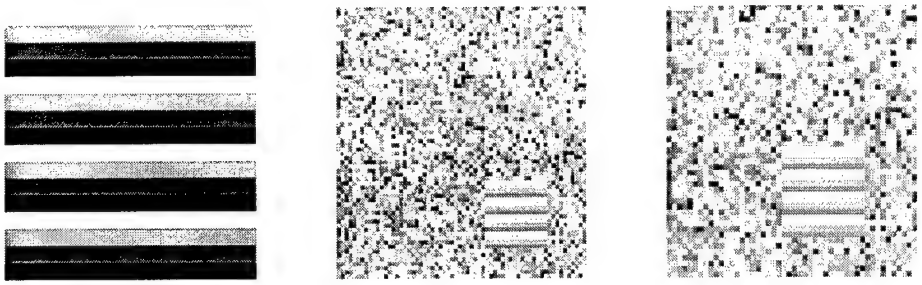


Figure 7.4.4 Figure 7.4.5 Figure 7.4.6

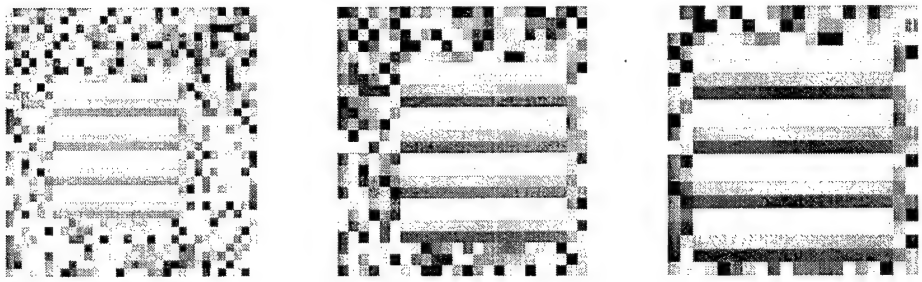


Figure 7.4.1. Pattern of horizontal bars of size 16×16.

Figure 7.4.2. Pattern in Figure 5.1 is placed in the scene of randomized magnitude of size 64×64. The placement is chosen randomly.

Figure 7.4.3. Based on the result of the first iteration of the projection of off-set coordinate of $(16, 16)$, the test image on coordinates $[16 : 63, 16 : 63]$ is displayed.

Figure 7.4.4. Based on the result of the second iteration of the projection of off-set coordinate of $(32, 32)$, the test image on coordinates $[32 : 63, 32 : 63]$ is displayed .

Figure 7.4.5. Based on the result of the second iteration of the projection of off-set coordinate of $(36, 32)$, the test image on coordinates $[36 : 59, 32 : 55]$ is displayed .

Figure 7.4.6. Based on the result of the second iteration of the projection of off-set coordinate of $(42, 39)$, the test image on coordinates $[42 : 61, 39 : 58]$ is displayed.

Location of noisy horizontal bars in random background

Figure 7.5.1 Figure 7.5.2 Figure 7.5.3

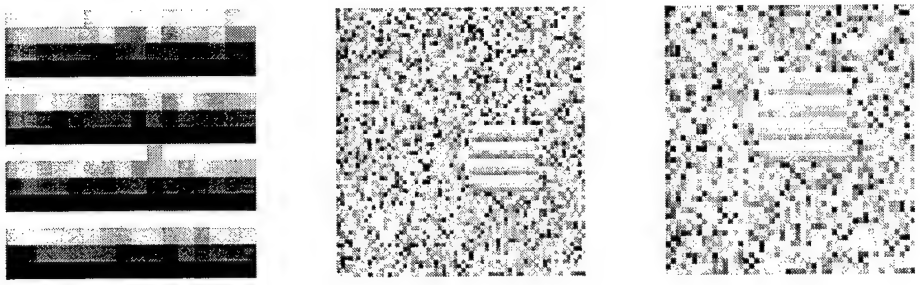


Figure 7.5.4 Figure 7.5.5 Figure 7.5.6

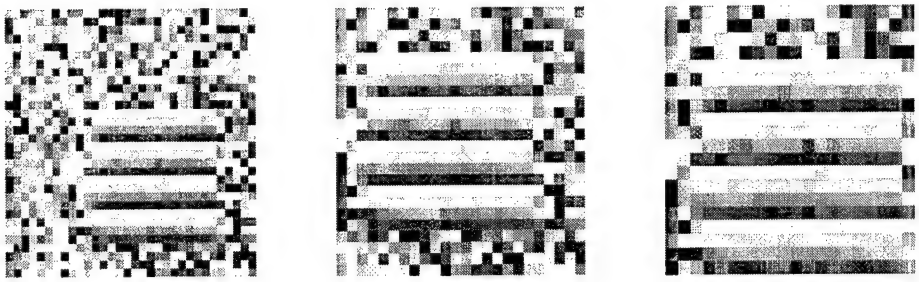


Figure 7.5.1. Pattern of noisy horizontal bars of size 16×16.

Figure 7.5.2. Pattern in Figure 6.1 is placed in the scene of randomized magnitude of size 64×64. The placement is chosen randomly.

Figure 7.5.3. Based on the result of the first iteration of the projection of off-set coordinate of $(16, 16)$, the test image on coordinates $[16 : 63, 16 : 63]$ is displayed.

Figure 7.5.4. Based on the result of the second iteration of the projection of off-set coordinate of $(16, 24)$, the test image on coordinates $[16 : 47, 24 : 55]$ is displayed .

Figure 7.5.5. Based on the result of the second iteration of the projection of off-set coordinate of $(24, 32)$, the test image on coordinates $[24 : 47, 32 : 55]$ is displayed .

Figure 7.5.6. Based on the result of the second iteration of the projection of off-set coordinate of $(24, 32)$, the test image on coordinates $[24 : 43, 32 : 51]$ is displayed.

7.2.2 Location of horizontal bars in random background

Figure 7.6.1 Figure 7.6.2 Figure 7.6.3

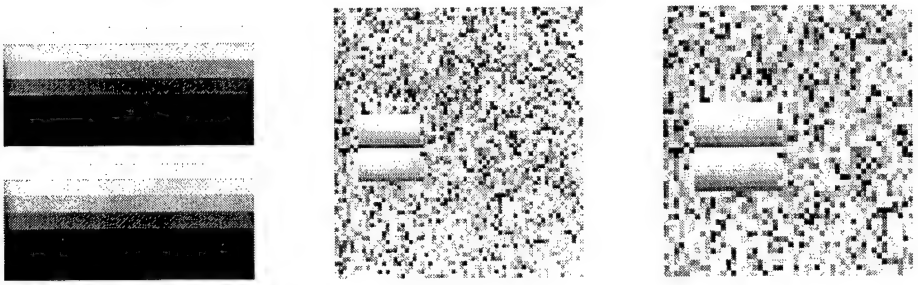


Figure 7.6.4 Figure 7.6.5 Figure 7.6.6

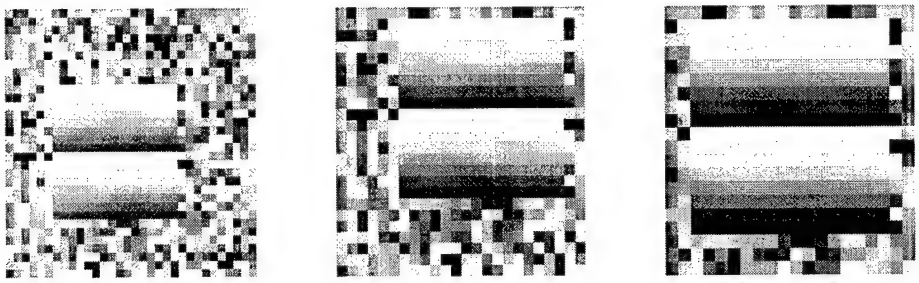


Figure 7.6.1. Pattern of noisy horizontal bars of size 16×16.

Figure 7.6.2. Pattern in Figure 7.1 is placed in the scene of randomized magnitude of size 64×64. The placement is chosen randomly.

Figure 7.6.3. Based on the result of the first iteration of the projection of off-set coordinate of $(8, 0)$, the test image on coordinates $[8 : 55, 0 : 47]$ is displayed.

Figure 7.6.4. Based on the result of the second iteration of the projection of off-set coordinate of $(16, 0)$, the test image on coordinates $[16 : 47, 0 : 31]$ is displayed .

Figure 7.6.5. Based on the result of the second iteration of the projection of off-set coordinate of $(24, 0)$, the test image on coordinates $[24 : 47, 0 : 23]$ is displayed .

Figure 7.6.6. Based on the result of the second iteration of the projection of off-set coordinate of $(24, 4)$, the test image on coordinates $[24 : 43, 4 : 23]$ is displayed.

Location of horizontal bars in pseudo-random background

Figure 7.7.1

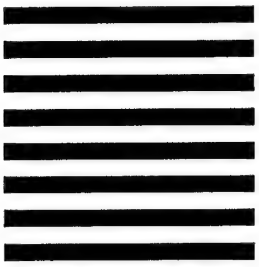


Figure 7.7.2

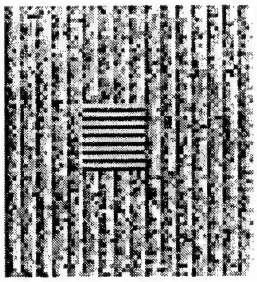


Figure 7.7.3

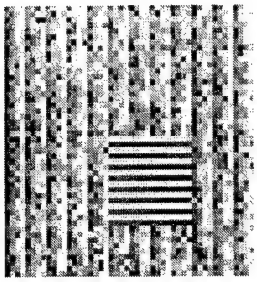


Figure 7.7.4

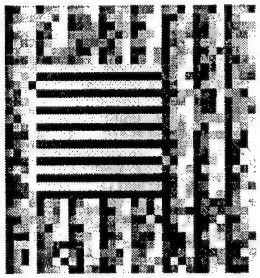


Figure 7.7.5

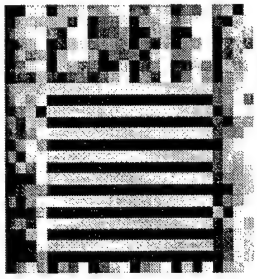


Figure 7.7.6

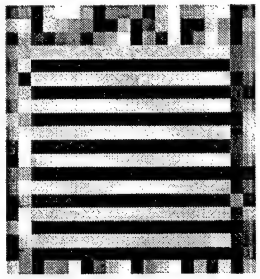


Figure 7.7.1. Pattern of horizontal bars of size 16×16.

Figure 7.7.2. Pattern in Figure 7.71 is placed in the somewhat structured scene of size 64×64. The placement is chosen randomly.

Figure 7.7.3. Based on the result of the first iteration of the projection of off-set coordinate of $(0, 0)$, the test image on coordinates $[0 : 47, 0 : 47]$ is displayed.

Figure 7.7.4. Based on the result of the second iteration of the projection of off-set coordinate of $(16, 16)$, the test image on coordinates $[16 : 47, 16 : 47]$ is displayed.

Figure 7.7.5. Based on the result of the second iteration of the projection of off-set coordinate of $(16, 16)$, the test image on coordinates $[16 : 39, 16 : 39]$ is displayed.

Figure 7.7.6. Based on the result of the second iteration of the projection of off-set coordinate of $(20, 18)$, the test image on coordinates $[20 : 39, 18 : 37]$ is displayed.

Location of horizontal bars in structured background

Figure 7.8.1

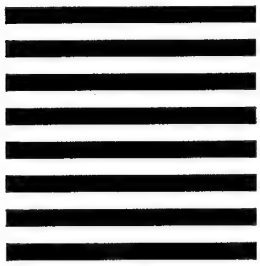


Figure 7.8.2

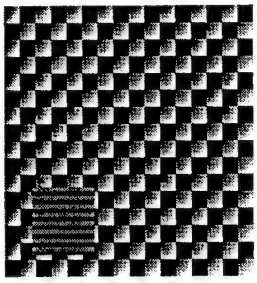


Figure 7.8.3

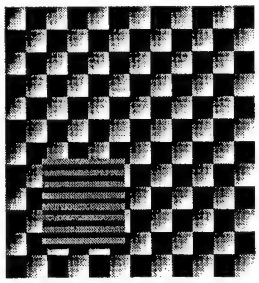


Figure 7.8.4

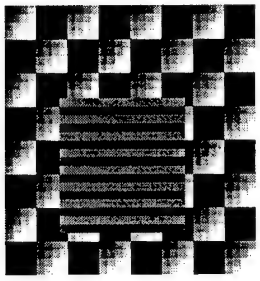


Figure 7.8.5

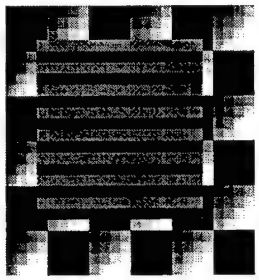


Figure 7.8.6

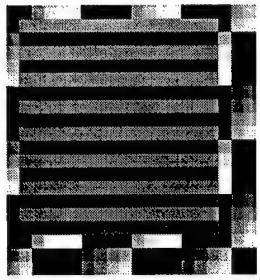


Figure 7.8.1. Pattern of horizontal bars of size 16×16.

Figure 7.8.2. Pattern in Figure 7.8.1 is placed in the somewhat structured scene of size 64×64. The placement is chosen randomly.

Figure 7.8.3. Based on the result of the first iteration of the projection of off-set coordinate of $(16, 0)$, the test image on coordinates $[16 : 63, 0 : 47]$ is displayed.

Figure 7.8.4. Based on the result of the second iteration of the projection of off-set coordinate of $(32, 0)$, the test image on coordinates $[32 : 63, 0 : 31]$ is displayed .

Figure 7.8.5. Based on the result of the second iteration of the projection of off-set coordinate of $(40, 4)$, the test image on coordinates $[40 : 63, 4 : 27]$ is displayed .

Figure 7.8.6. Based on the result of the second iteration of the projection of off-set coordinate of $(42, 6)$, the test image on coordinates $[42 : 63, 6 : 25]$ is displayed.

Location of horizontal bars in pseudo-structured background

Figure 7.9.1 Figure 7.9.2 Figure 7.9.3

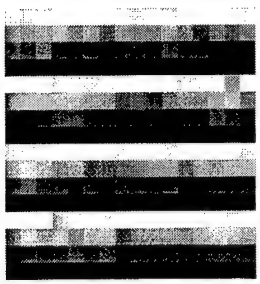
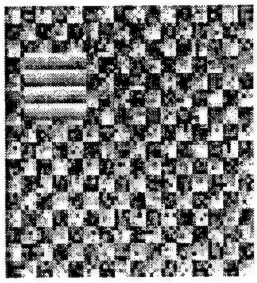
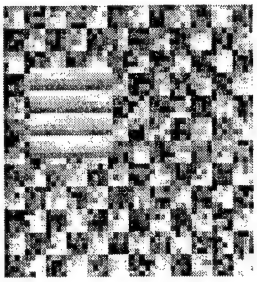




Figure 7.9.4 Figure 7.9.5 Figure 7.9.6

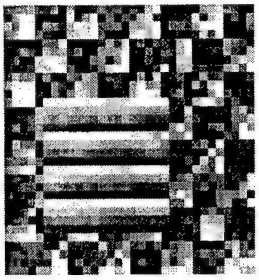
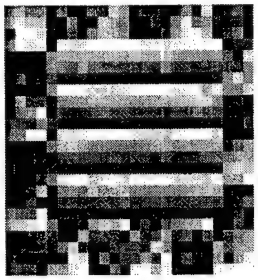
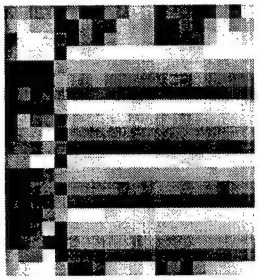




Figure 7.9.1. Pattern of horizontal bars of size 16×16.

Figure 7.9.2. Pattern in Figure 7.9.1 is placed in the somewhat structured scene of size 64×64. The placement is chosen randomly.

Figure 7.9.3. Based on the result of the first iteration of the projection of off-set coordinate of $(0, 0)$, the test image on coordinates $[0 : 47, 0 : 47]$ is displayed.

Figure 7.9.4. Based on the result of the second iteration of the projection of off-set coordinate of $(0, 0)$, the test image on coordinates $[0 : 31, 0 : 31]$ is displayed .

Figure 7.9.5. Based on the result of the second iteration of the projection of off-set coordinate of $(8, 0)$, the test image on coordinates $[8 : 31, 0 : 23]$ is displayed.

Figure 7.9.6. Based on the result of the second iteration of the projection of off-set coordinate of $(8, 0)$, the test image on coordinates $[8 : 27, 0 : 19]$ is displayed.

Location of horizontal bars in pseudo-structured background

Figure 7.10.1 Figure 7.10.2 Figure 7.10.3

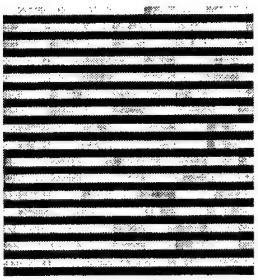
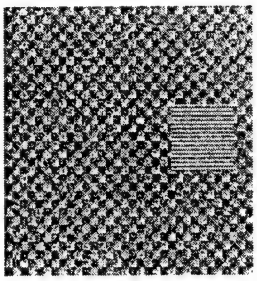
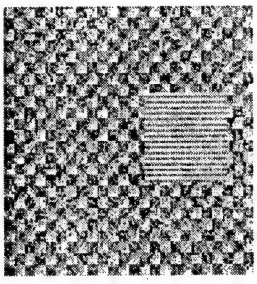




Figure 7.10.4 Figure 7.10.5 Figure 7.10.6

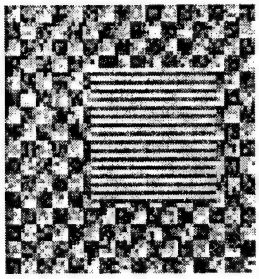
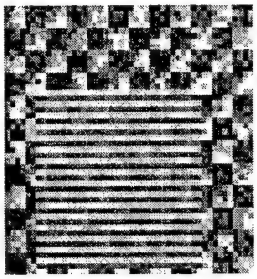
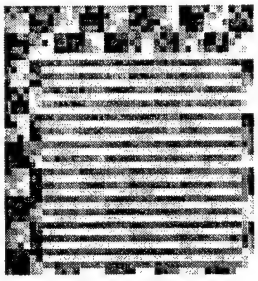




Figure 7.10.1. Pattern of horizontal bars of size 32×32.

Figure 7.10.2. Pattern in Figure 7.10.1 is placed in the somewhat structured scene of size 128×128. The placement is chosen randomly.

Figure 7.10.3. Based on the result of the first iteration of the projection of off-set coordinate of $(16, 32)$, the test image on coordinates $[16 : 111, 32 : 127]$ is displayed.

Figure 7.10.4. Based on the result of the second iteration of the projection of off-set coordinate of $(32, 64)$, the test image on coordinates $[32 : 95, 64 : 127]$ is displayed .

Figure 7.10.5. Based on the result of the second iteration of the projection of off-set coordinate of $(32, 80)$, the test image on coordinates $[32 : 79, 80 : 127]$ is displayed .

Figure 7.10.6. Based on the result of the second iteration of the projection of off-set coordinate of $(41, 81)$, the test image on coordinates $[41 : 80, 81 : 120]$ is displayed.

7.3 Software for automatic location of targets

7.3.1 The problem

Dr. Albanese (210-536-5710) at Brooks AFB has posed the problem of detecting and locating rectangles in severe noise: the level of noise is such that the rectangles are hardly recognizable.

Several of the previously implemented nonabelian group filters project line segments in somewhat noisy, cluttered background. Digitally recorded rectangles are viewed as several line segments of the same lengths occupying some consecutive pixels in the direction perpendicular to the line segments. As the noise level increases, and the size of the object reduces, the projections become less robust.

7.3.2 A solution

Imaging model

In general, an imaging model for an image of size $N \times N$, $N = 2^K$, is based on

- A semi-direct product group $A \leftthreetimes B$ of order N^2 where A and B are abelian groups,
- An indexing of the image by the group.

For reasons explained more fully in the next section, we choose A and B so that

- $A = \mathbf{Z}/2^M \times \mathbf{Z}/2^M$, $M = K - 2$.
- B is a subgroup of $GL(2, 2^M)$ isomorphic to

$$C_2 \times C_2 \times C_2 \times C_2,$$

  where C_2 is the cyclic group of order 2.

We have previously (Report 3, January 2001) investigated various actions of $GL(2, 2^M)$ on A. To construct subgroups B of this form, we need to find four commuting elements of order 2 in $GL(2, 2^M)$.

By an action of B on A, we always mean a semi-direct product action. For a fixed action of B on A, the indexing of the image by $A \leftthreetimes B$ is given as in the table.

b_0A	b_1A	b_2A	b_3A
b_4A	b_5A	b_6A	b_7A
b_8A	b_9A	$b_{10}A$	$b_{11}A$
$b_{12}A$	$b_{13}A$	$b_{14}A$	$b_{15}A$

Table 1. Ordering of $A \leftthreetimes B$

The indexing of $B = \{1 = b_0, b_1, \ldots, b_{15}\}$ will have no effect on the resulting processing.

The design problem is to construct an action of B on A such that relative to the specified indexing some translation invariant subspace in the group algebra $\mathbf{C}(A \leftthreetimes B)$ will contain

lines in the image at a prescribed orientation. From the general theory, the solution to this problem is given by studying the induced action of B on the set of characters A^* viewed as a subset of $\mathbf{C}(A \not\triangleleft B)$. First index A by (k_1, k_2), $0 \leq k_1, k_1 < 2^M$ and consider A as ordered lexicographically. The set of characters A^* is indexed by (l_1, l_2), $0 \leq l_1, l_2 < 2^M$, where the character α_{l_1,l_2} is defined by

$$\alpha_{l_1,l_2}(k_1, k_2) = e^{2\pi i \frac{l_1 k_1 + l_2 k_2}{2^M}}.$$

A^* is ordered lexicographically as well.

Suppose the design problem is to choose an action of B on A such that a line of slope $-c$ in the image is contained in some translation invariant subspace associated to $A \not\triangleleft B$ in $\mathbf{C}(A \not\triangleleft B)$. To solve this problem we must choose an action of B on A such that the induced action of B on A^* satisfies the property that there exists a $b \in B$ such that in $\mathbf{C}(A \not\triangleleft B)$,

$$b\alpha_{cl_1,l_1} = \alpha_{cl_1,l_1} b, \quad 0 \leq l_1 < 2^M.$$

This is equivalent to the assertion that the centralizer subgroup in $\mathbf{C}(A \not\triangleleft B)$ of the line of characters, α_{cl_1,l_1}, $0 \leq l_1 < 2^M$, is nontrivial. For the prescribed orientation of the lines in the image of the project described above, the developed software implements actions of B on A solving the design problem.

This software has another feature which we have found is especially important. There may be many actions of B on A which solve the design problem. For producing the most robust (in noise or clutter) filtering of images for detecting of lines at prescribed orientations, we have found that some are better than others based on the following criterion.

Fix an action θ of B on A and form the resulting semi-direct product $A \not\triangleleft_\theta B$. For a line of characters and a subgroup C of B, let $n(C, \theta)$ be number of characters in the line centralized by C in $\mathbf{C}(A \not\triangleleft_\theta B)$. As C runs over the subgroups of B, the numbers $n(C, \theta)$ may vary. Denote the largest by $n(\theta)$. As θ runs over the actions of B on A, the numbers $n(\theta)$ may vary. We have found that actions θ of B on A producing the largest $n(\theta)$ will yield the most robust (in noise or clutter) detection of lines of slope $-c$.

Choice of the order of A

In general the relative orders of A and B in the indexing of an image by $A \not\triangleleft B$ affects the localization properties of the resulting nonabelian group filtering operations. There is an ambiguity of location determined by the size of A, the smaller the order of A,the smaller the ambiguity. In the ideal case, the size of the object should be the same as the order of A. This has the following consequence for the specific design problem considered in the project describe above.

The line defined by a pair $(-l_2, l_1)$ in A is an algebraic line of length 2^M. An image containing a geometric line segment of the same slope will have a large coefficient in its orthogonal idempotent expansion. Although this property completely localizes the geometric line segment in the direction (l_1, l_2), there are ambiguities in determining the length and position of the line segment upto the order of A. A should be chosen so that the lines in A have the same order as the geometric line segment: ambiguity in a few pixels can be resolved

by other criteria. In noise-free images, the relative magnitudes of the expansion coefficients exactly determine the length of a line segment.

Software tool for detection/localization

The software tool incorporates projection operators from three different realizations of

$$C_2 \times C_2 \times C_2 \times C_2,$$

to mitigate clutter and noise. One such realization is given as the group generated by

$$\begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 2^M \\ 2^M & 1 \end{bmatrix}, \quad \begin{bmatrix} 2^M - 1 & 0 \\ 2^M & 2^M - 1 \end{bmatrix}.$$

Each of the three realizations of B contains the element

$$b = \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix}.$$

Observe that $b \in B(\alpha_{0,l_1})$, $0 \leq l_1 < 2^M$.

The software tool processes an image of size 128×128 by projecting the image into orthogonal invariant subspaces of $\mathbf{C}(A \triangleleft B)$, using the three different realizations of B. The location of the maximal coefficients in the spaces spanned by

$$\tau\alpha_{cl_1,l_1}, \quad 0 \leq l_1 < 2^M, \tau \in B(\alpha_{cl_1,l_1})^*$$

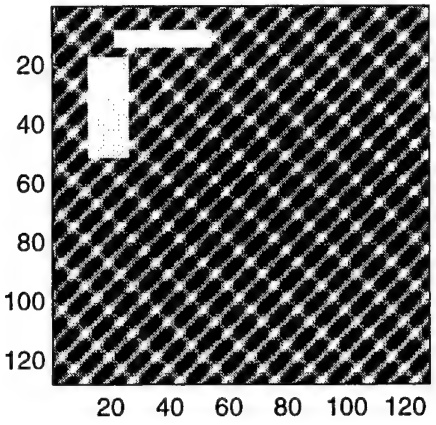
are compared. If the locations of the maximal coefficients from the three distinct projections are the same, and the y-coordinate is produced and the confidence level is set to 3 (out of 0, 1, 2, and 3). This is due to the fact that the three distinct projections behave differently in the presence of randomized white noise. If such locations differ by less than the width of the object of interest, the weighted-average location is produced as the y-coordinate and confidence level is reduced from 3 by 1 or 2 depending on the values and the locations of the maximal coefficients.

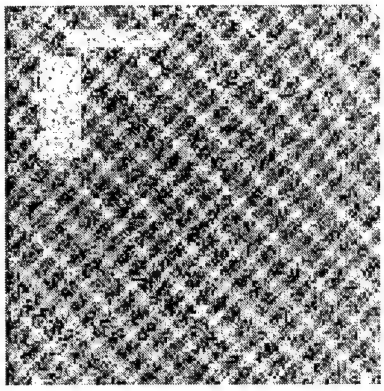
To localize the x-coordinate as well as the length of the object, parameterized thresholding of the projection coefficients is used. Again, depending the number of matches in the three different projections, x-coordinate, the length of the object and updated confidence level is produced.

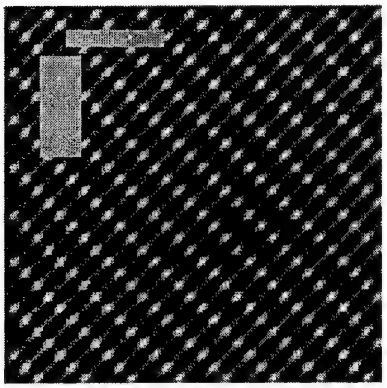
7.3.3 Example scenes

All the figures in this report are log-scaled, gray scale, intensity plots. In each set of three images, the image on top left is the noise-free scene consisting of two rectangular boxes in structured background. The rectangular boxes vary in sizes up to 4 pixels in each direction, and placed at random in the scene. The intensity of the structured background is 120% of the intensity of the boxes. The image on top right is the result of adding white noise to the scene on top left and is used as input to processing. The software tool automatically

produces the coordinates of the centers of the two boxes along with a confidence level. The first component of the ordered pair indicating the coordinate is the vertical distance from the top of the image, while the second component is the horizontal distance from the left. The image on bottom left is the noise-free scene with the resulting coordinates highlighted. The purpose of this is to show the positions of the computed coordinates relative to the original scene.

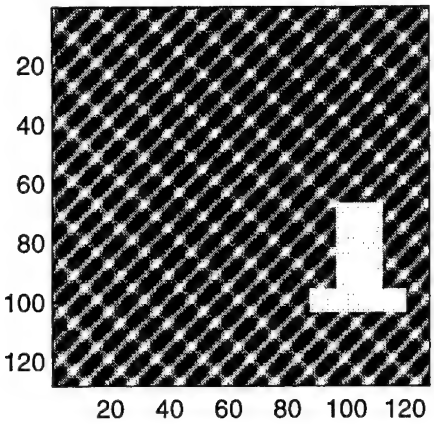


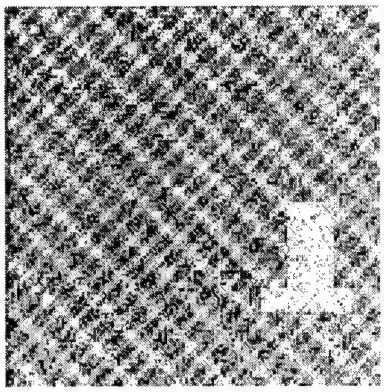


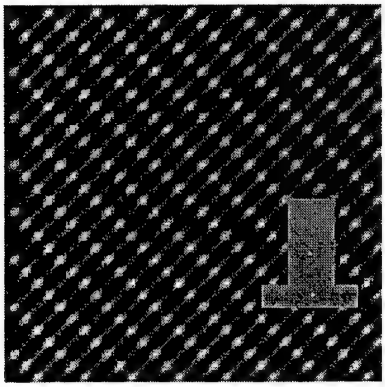


vertical box, centered at (25,19), c-level= 3

horizontal box, centered at (11,43), c-level= 3

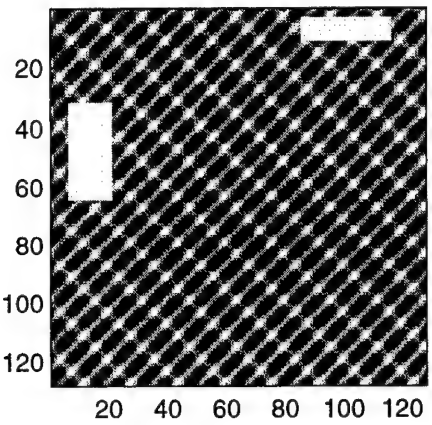


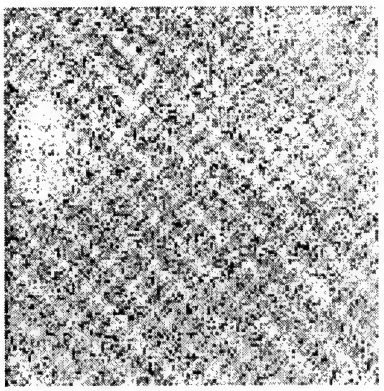


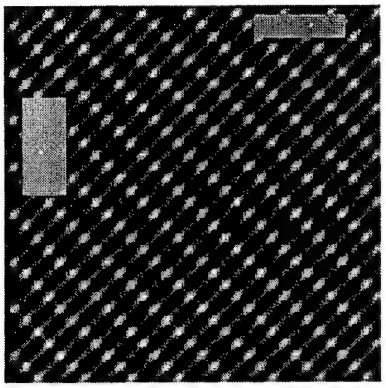


vertical box, centered at (85,104), c-level= 3

horizontal box, centered at (99,105), c-level= 3

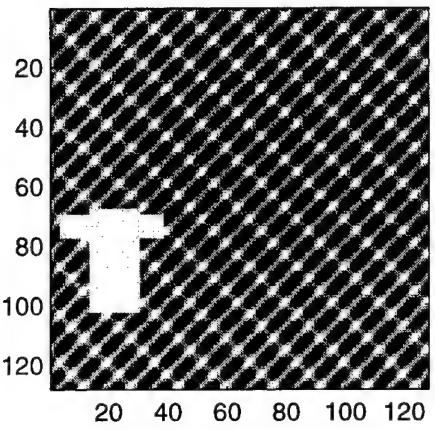


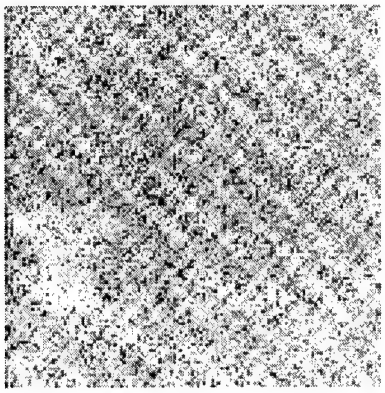


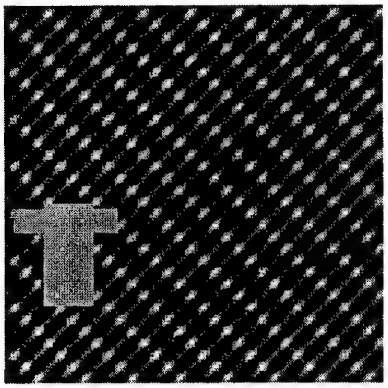


vertical box, centered at (50,13), c-level= 3

horizontal box, centered at (7,105), c-level= 3

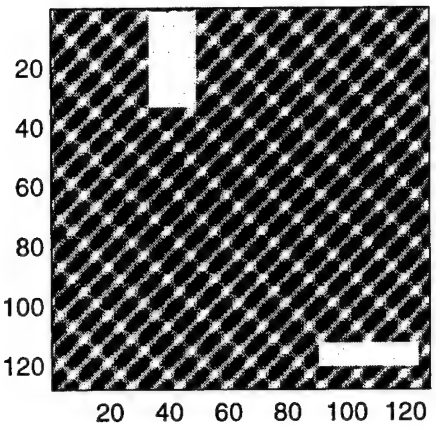


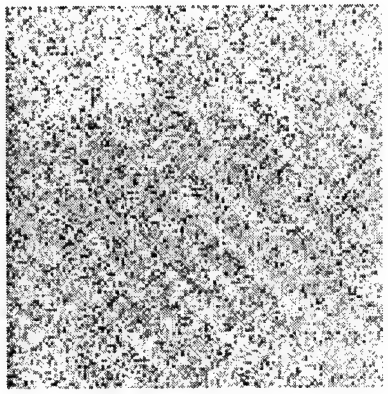


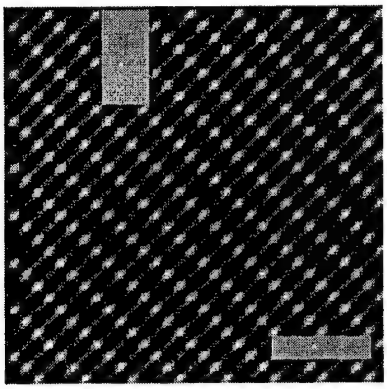


vertical box, centered at (83,20), c-level= 1

horizontal box, centered at (99,18), c-level= 2

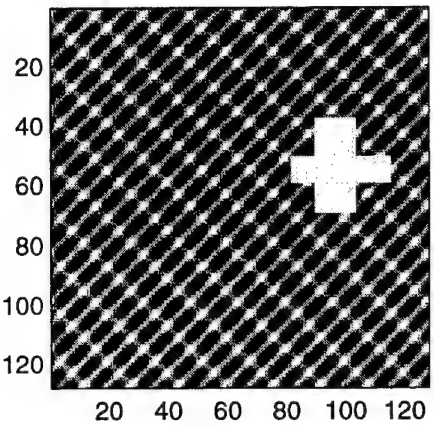


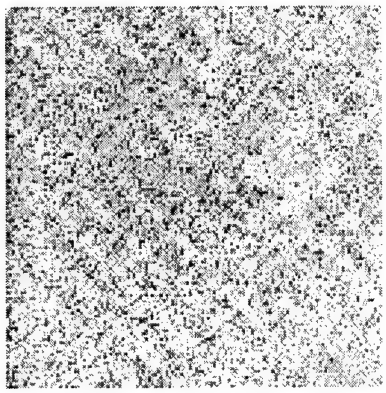


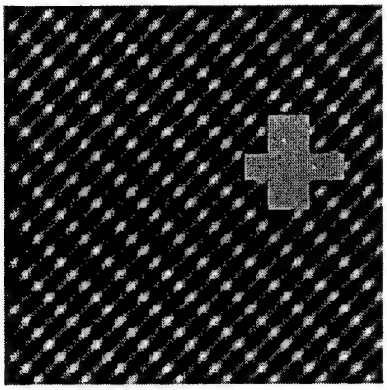


vertical box, centered at (20,40), c-level= 3

horizontal box, centered at (116,105), c-level= 1

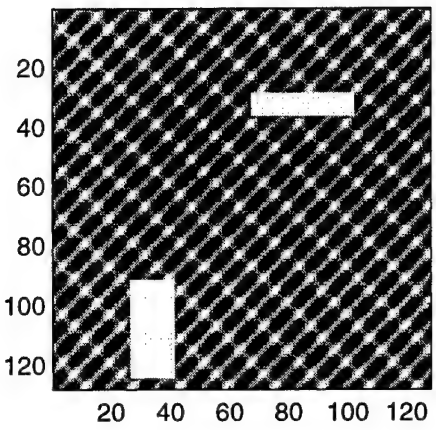


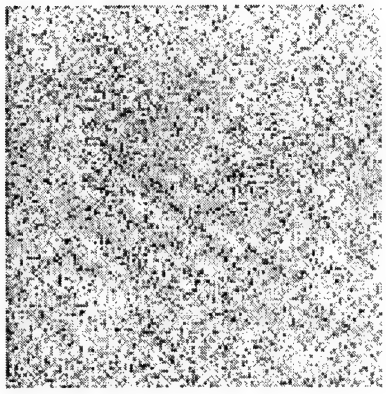


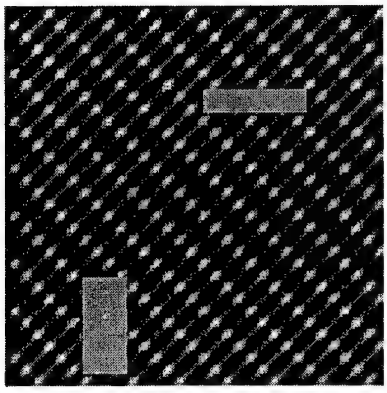


vertical box, centered at (46,95), c-level= 3

horizontal box, centered at (55,105), c-level= 1

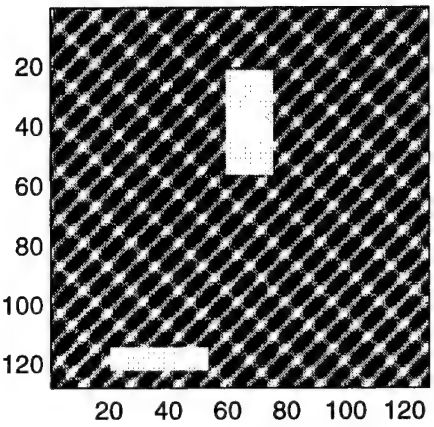


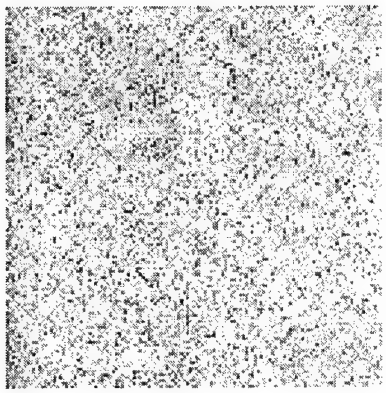


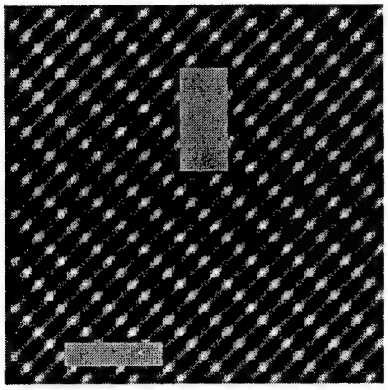


vertical box, centered at (105,34), c-level= 3

horizontal box, centered at (106,25), c-level= 0

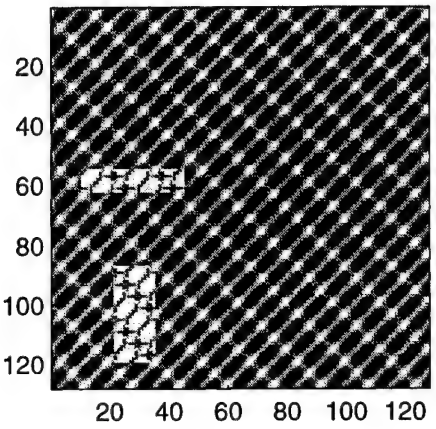


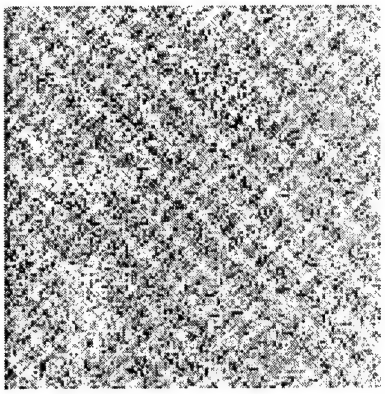


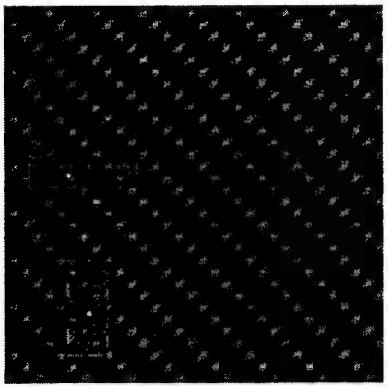


vertical box, centered at (45,77), c-level= 0

horizontal box, centered at (118,64), c-level= 3

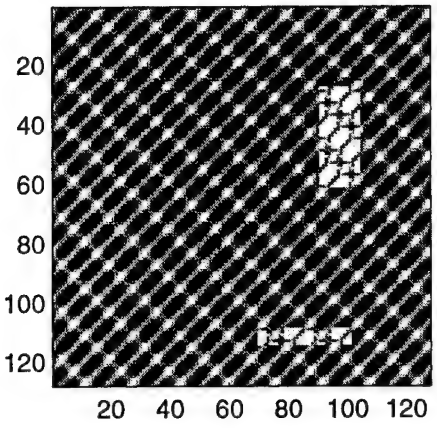


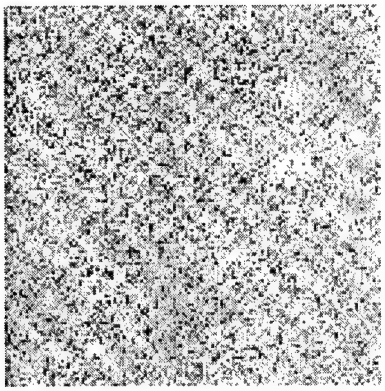


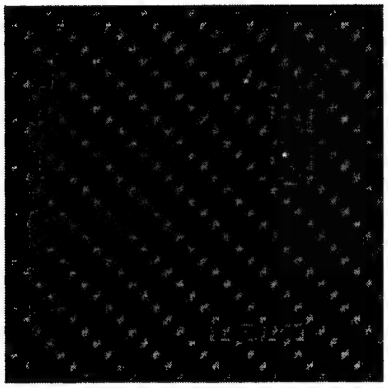


vertical box, centered at (105,29), c-level= 3

horizontal box, centered at (58,22), c-level= 3

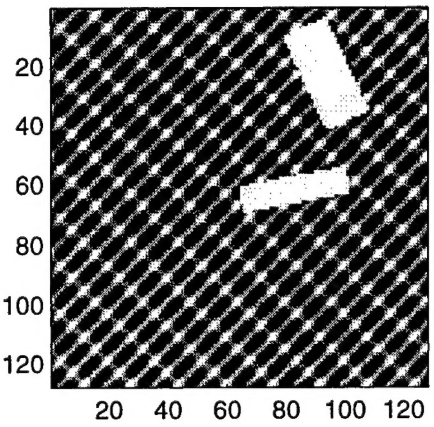


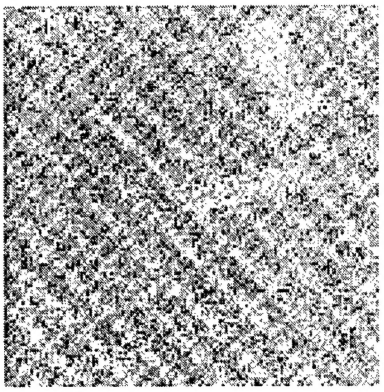


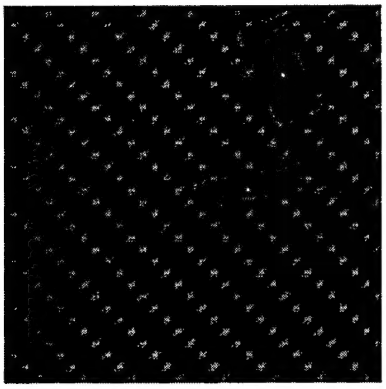


vertical box, centered at (51,95), c-level= 3

horizontal box, centered at (26,82), c-level= 1

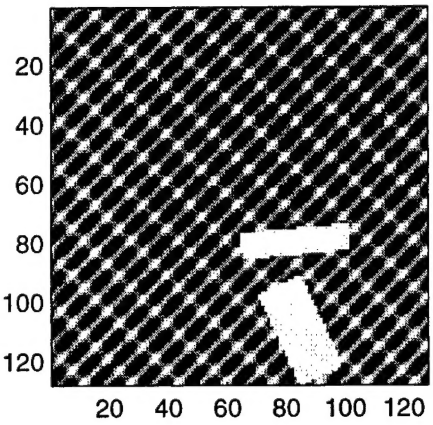


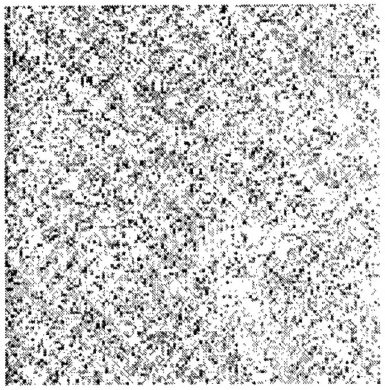


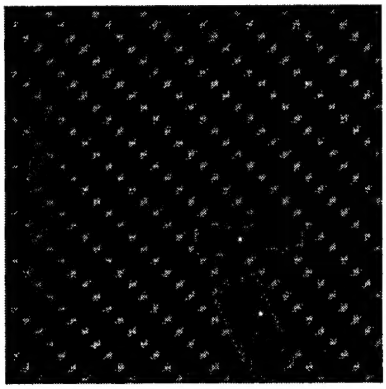


thick box, centered at (24,95), c-level= 3

thin box, centered at (63,83), c-level= 3







thick box, centered at (105,87), c-level= 3

thin box, centered at (80,80), c-level= 3

References

[1] L. Auslander and R. Tolimieri, "Is computing with the finite Fourier transform pure or applied mathematics?," *Bull. Math. Soc.(N.S.)* **1**(6), 847-897, 1997.

[2] U. Baum, "Existence and efficient construction of fast Fourier transforms for supersolvable groups," *Computational Complexity* **1**, 235-256, 1991.

[3] U. Baum, M. Clausen and B. Tietz, "Improved upper complexity bounds for the discrete Fourier transform," *AAECC* **2**, 35-43, 1991.

[4] R. Blahut, *Algebraic methods for signal processing and communications coding,* Springer-Verlag, NY 1992.

[5] L. Beckett and P. Diaconis, "Spectral analysis for discrete longitudinal data," *Adv. Math.* **103** 1994, 107-128.

[6] T.C. Carins, "On the Fourier transform on finite abelian groups'" *IEEE Trans., Comput.*, 569-671, May 1971.

[7] J.W. Cooley and J.W. Tukey, "An algorithm for machine calculation of complex Fourier series," *Math. Comp.*, **19**, 297-301, 1965.

[8] P. Diaconis, "A Generalization of spectral analysis of with applications to ranked data," *Ann. Stat.* **17**, 949-979, 1989.

[9] P. Diaconis, *Group representations in probability and statistics*, IMS, Hayward, CA, 1988.

[10] P. Diaconis and D. Rockmore, "Efficient computation of the Fourier transform on finite groups," *J. of AMS* **3**(2), 297-332, 1990.

[11] D. Eberly and D. Wenzel, "Adaptation of group algebras to signal and image processing," *CVGIP: Graphical models and image processing* **53**(5), 1689-1711, 1996.

[12] A. Figá-Talamanca and C. Nebbia, "Harmonic analysis and representation theory for groups acting on homogeneous tress," *LMS Lecture note series 162,* Cambridge U. Press, 1991.

[13] Y. Fisher, E.W. Jacobs and R.D. Boss, "Fractal image compression using iterated transforms," *Image and text compression*, J. Storer, ed., 35-61, Kluwer Academic Press.

[14] R. Holmes, "Signal processing on finite groups," *Technical Report 873*, MIT Lincoln Laboratory, 1990.

[15] R. Holmes, "Mathematical foundations of signal processing II," *Technical Report 781*, MIT Lincoln Laboratory, 1987.

[16] T.A.C.M. Kalker and L.A. Shah, "A group theoretic approach to multidimensional filter banks: theory and applications," *IEEE Trans. SP* **44**(6), 1392-1405, 1996.

[17] M. Karpovski, "Fast Fourier transforms on finite nonabelian groups," *IEEE Trans. Comput.*, **C-26**(10), 1028-1030, 1977.

[18] M. Karpovski and E. Trachtenberg, "Filtering in a communication channel by Fourier transforms over finite groups," *Spectral techniques and fault detection*, M. Karpovski, ed., Academic Press, NY 1985.

[19] R. Lenz, "Using representations of the dihedral groups in the design of early vision filters," *Proc. ICASSP* **5**, 165-168, 1993.

[20] R. Lenz, *Group theoretical methods in image processing* Springer-Verlag, NY 1987.

[21] F.J. MacWilliams, "Codes and ideals in group algebras," *Combinatorial mathematics and its applications*, 317-328, R.C. Bose and T.A. Dowlin, eds., University of North Carolina Press, Chapel Hill, 1969.

[22] D. Maslen and D. Rockmore, "Generalized FFTs'" *DIMACS Ser. in Disc. Math. and Theor. Comp. Sci.,* **28**, 183-237, L. Finkelstein and W. Kantor, eds., 1997.

[23] D. Maslen and D. Rockmore, "Separation of variables and the efficient computation of Fourier transforms on finite groups, I," *J. of AMS* **10**(1), 169-214, 1997.

[24] G. Mirchandani , R. Foote, D. Rockmore, D. Healy and T. Olson, "A wreath product group approach to image processing,", in preparation.

[25] H.J. Nussbaumer, *Fast Fourier transform and convolution algorithms*, 2nd ed., Springer-Verlag, Berlin, 1982.

[26] J.P. Serre, *Linear representation of finite groups*, Springer-Verlag, NY, 1977.

[27] S. Winograd, "Arithmetic complexity of computations," *CBMS-NSF Regional Conf. Ser. Appl. Math., SIAM* **33**, 1980.